

Edmerson Arrigo Duarte Vaz

Segurança dos Sistemas de Informação

Estudo de Caso INPHARMA

Universidade Jean Piaget de Cabo Verde

Campus Universitário da Cidade da Praia
Caixa Postal 775, Palmarejo Grande
Cidade da Praia, Santiago
Cabo Verde

2.9.14

Edmerson Arrigo Duarte Vaz

Segurança dos Sistemas de Informação

Estudo de Caso INPHARMA

Universidade Jean Piaget de Cabo Verde

Campus Universitário da Cidade da Praia
Caixa Postal 775, Palmarejo Grande
Cidade da Praia, Santiago
Cabo Verde

2.9.14

Edmerson Arrigo Duarte Vaz, autor da monografia intitulada: Segurança dos Sistemas de Informação, declaro que, salvo fontes devidamente citadas e referidas, o presente documento é fruto do meu trabalho pessoal, individual e original.

Cidade da Praia, aos 2 de Setembro de 2014
Edmerson Arrigo Duarte Vaz

Memória Monográfica apresentada à Universidade Jean Piaget de Cabo Verde como parte dos requisitos para a obtenção do grau de Licenciatura em Informática de Gestão

Sumário

Atualmente, a segurança dos sistemas da informação das organizações, são cada vez mais colocados à prova por diversos tipos de ameaças de diversificadas origens, onde se incluem as tão frequentes fraudes eletrónicas, nomeadamente a espionagem, sabotagem, vandalismo, *hackers* e ataques DoS, que se tornam cada vez mais sofisticados e ambiciosos.

A dependência dos sistemas e serviços de informação, leva a crer que as organizações estão cada vez mais vulneráveis às ameaças de segurança. O uso simultâneo de redes públicas e privadas e a partilha de recursos de informação, são fatores que contribuem para o acréscimo da dificuldade em se controlar os acessos, e a respetiva segurança dos mesmos.

Para dar a conhecer a Segurança de Sistema de Informação, foi elaborado um estudo de caso na Inpharma, baseada nas melhores práticas do mercado, orientado pela norma ISO/IEC 27002:2005, que rege os padrões internacionais da segurança da informação, de modo a identificar o nível de segurança SI, face ao nível de risco identificado, auxiliando a definição dos próximos passos evolutivos da segurança dos Sistemas e da Informação, com o objetivo de redução de risco de segurança, com base em referências que aproxime gradualmente o nível de segurança praticado, aos níveis adequados ao negócio.

Por conseguinte dado a importância da Segurança do Sistema de Informação, é indispensável que as medidas devem ser adotadas de forma a minimizar os impactos que podem causar a organização.

Palavras – chaves: Segurança Informática, Sistemas de Informação, Planeamento de Segurança.

Dedicatória

*Á minha mãe, Maria Sameiro Duarte dos Reis pela confiança
e sacrifício.*

Agradecimentos

Este trabalho foi concretizado graças ao apoio de inúmeras pessoas que direta ou indiretamente deram algum contributo para que tal acontecesse, por isso, manifesta-se agradecido a todas essas pessoas, mas considera-se pertinente particularizar as seguintes:

Ao meu orientador, Eng.º Stefan Monteiro, por estimular o meu interesse pelo conhecimento, pela vida académica, e participação ativa no desenvolvimento desta pesquisa.

Ao meu amigo, Fernando Monteiro pelo acompanhamento e apoio nesta jornada, dando sempre sugestões e correções, bem como pelas suas ideias então demonstradas.

Deixei para o fim a todos uma única palavra:

Obrigado!

Conteúdo

Introdução	7
Justificação do Tema	9
Objetivo Geral	9
Objetivos Específicos	9
Metodologia.....	10
Estrutura do trabalho	10
 Capítulo 1: Segurança dos Sistema de Informação	 12
1 Conceito de Segurança do Sistema de Informação	12
2 Ameaças	14
3 Análise de Risco	18
3.1 Sistema de Gestão de Risco.....	23
4 Áreas da Segurança da Informação	29
4.1 Segurança Física	29
4.1.1 Equipamentos	32
4.1.2 Instalações	34
4.2 Segurança do Pessoal	35
4.2.1 Recrutamento e Mudança de Contratação	36
4.2.2 Sensibilização e Formação	37
4.3 Segurança Logica	38
4.3.1 Autenticação e Controlo de Acesso.....	39
4.3.2 Redundância	40
4.3.3 Criptografia.....	41
4.3.4 Assinatura Digital	45
4.3.5 Antivírus	46
4.3.6 Filtragem de Conteúdos.....	47
4.3.7 Salvaguarda da Informação	47
4.3.8 Deteção de Intrusões.....	51
4.3.9 Resposta a ataques	53
4.4 Testes e Auditorias	55
5 Segurança face ao desastre	57
 Capítulo 2: Plano Global de Segurança.....	 59
1 Plano de Segurança.....	59
1.1 Plano de Contingência	60
1.2 Plano de Recuperação.....	62

1.3	Plano de Reposição.....	63
1.4	Política de Segurança	64
1.5	Normas de Segurança	67
1.6	Procedimentos	70
Capítulo 3: O Caso INPHARMA		71
1	Enquadramento	71
2	Apresentação da INPHARMA	72
3	Missão, Visão e Valores	74
3.1	Missão.....	74
3.2	Visão.....	74
3.3	Valores.....	75
4	Estrutura Organizacional	76
5	Infraestrutura das TIC.....	77
6	Arquitetura de Rede.....	79
7	Backup & Restauro.....	81
8	Medidas de Segurança do SI na INPHARMA	83
9	Análise dos Resultados.....	85
9.1	Segurança Física	86
9.2	Segurança com Recursos Humanos.....	88
9.3	Segurança Lógica	90
10	Proposta de Política Mesa Limpa e Proteção de Ecrã	92
11	Proposta de Política de Sensibilização e Formação.....	94
12	Proposta de Política de Manutenção e Utilização dos Equipamentos	96
Conclusão		98
Bibliografia.....		100
Anexo		i
A.1	Declaração de Confidencialidade INPHARMA.....	i
Apêndices.....		ii
I.	Checklist proposto para verificação da Segurança Física baseado na norma ABNT NBR ISO/IEC 27002	iii
II.	Checklist proposto para verificação da Segurança dos Recursos Humanos baseado na norma ABNT NBR ISO/IEC 27002	v
III.	Checklist proposto para verificação da Segurança Lógica baseado na norma ABNT NBR ISO/IEC 27002	vi

Tabelas

Tabela 1: Fatores e grau de risco, adaptado (Carneiro, 2002)	19
Tabela 2: Alinhamento do processo do SGSI e do processo de gestão de riscos de segurança da informação, adaptado (ISO/IEC 27005:2008)	28
Tabela 3: Segurança Física, adaptado de (Carneiro, 2002).	30
Tabela 4: Activos de tecnologias e sistemas de informação da Inpharma	78
Tabela 5: Segurança Física	87
Tabela 6: Segurança de Recursos Humanos	89
Tabela 7: Segurança Logica	91

Figuras

Figura 1: Regras Baseadas no Mapa de risco	22
Figura 2: Etapas do Sistema de Gestão de Riscos da Segurança da Informação	23
Figura 3: Modelo PDCA aplicado aos processos do SGSI	27
Figura 4: Infraestrutura redundante – Exemplo (Silva, Carvalho e Torres, 2003).....	41
Figura 5: Criptografia Simétrica com uso de uma Única Chave, adaptado de (Moraes, 2010)	43
Figura 6: Criptografia Assimétrica, adaptado de (Moraes, 2010)	44
Figura 7: Diagrama de execução	62
Figura 8: Modelo de formulação da política de segurança, adaptado (Ferreira e Alves ,1995)	66
Figura 9: ABNT NBR ISO/IEC 27002:2005 - Estrutura (Pompeu, Gledson, 2010)	69
Figura 10: Edifício – Bloco Administrativo dos Laboratórios INPHARMA.....	72
Figura 11: Historial INPHARMA	73
Figura 12: Missão, Visão, Valores da INPHARMA	75
Figura 13: Organograma da INPHARMA	76
Figura 14: Arquitetura de rede INPHARMA	80
Figura 15: Mensagem de notificação de alerta do estado de backup	82

Siglas/Abreviaturas

ABNT - Associação Brasileira de Normas e Técnicas

ADSL - Asymmetric Digital Subscriber Line

AES - Padrão de Criptografia Avançada

ANAC – Agencia Nacional de Comunicações

BS – British Standard

CNASI - Congresso de Segurança da Informação, Auditoria e Governança da TIC

COBIT - Objectives for Information and related Technology

DE – Direção Executiva

DES - Data Encryption Standard

DOS – Denial of Service

HIDS - Host-based Intrusion Detection System

IOT - International Organization for Standardization

ISACA - Information Systems Audit and Control Association

ISO - International Standards Organization

NIDS - Netwok Intrusion Detection System

PDCA – Planear, Inplementar, Verificar, Agir

PIN - Personal Identification Number

RAID - Redundant Array of Unresponsive Disks

RC2 - Encryption Algorithm

RSA – Rivest, Chamir e Adleman

SGRSI – Sistema de Gestão de Riscos da Segurança da Informação

SI - Sistemas de Informação

SSI - Segurança de Sistema de Informação

TI - Tecnologias de Informação

TIC - Tecnologias de Informação e Comunicação

UPS - Uninterruptible Power Supply

URL - Uniform Resource Locator

VPN - Virtual Private Network

3DES - Triple Data Encryption Standard

Introdução

As necessidades e exigências associadas à realidade empresarial do mercado atual, implica que a plataforma de Tecnologias e Sistemas de Informação garantam índices de segurança, a nível da confidencialidade, disponibilidade e integridade extremamente elevados.

Nesse sentido, e independentemente da dimensão ou área de negócio das empresas, existe um fator comum e fundamental para o sucesso de qualquer organização que sustente o seu “core business” sobre Sistemas de Informação: a garantia de segurança da informação, qualidade e estabilidade dessa mesma plataforma tecnológica.

Os incidentes de segurança da informação vêm aumentando consideravelmente ao longo dos últimos anos e assumem as formas mais variadas, como, por exemplo: infeção por vírus, acesso não autorizado, ataques DoS contra redes e sistemas, furto de informação proprietária, invasão de sistemas, fraudes internas e externas, uso não autorizado de redes sem fio, entre outras.

Juntamente com a difusão da Internet, outros fatores contribuíram para impulsionar o crescimento dos incidentes de segurança. Um desses fatores é o aumento do número de vulnerabilidades nos sistemas existentes, como, por exemplo, as brechas de segurança nos sistemas operacionais utilizados em servidores e postos de trabalho. Outro fator é o quão trabalhoso e custoso pode se tornar o processo de mitigar tais vulnerabilidades com a aplicação de correções do sistema, realizadas muitas vezes de forma manual e individual: de máquina em máquina. Por último, a complexidade e a sofisticação dos ataques também contribuíram de maneira direta para o aumento dos incidentes.

É a conjunção dessas condições que culmina, por exemplo, na parada generalizada de sistemas e redes corporativas ao redor do mundo, causada pela atuação de *worms* que se propagam pela Internet em questão de minutos. A tendência é que as ameaças à segurança continuem a crescer não apenas em ocorrência, mas também em velocidade, complexidade e alcance, tornando o processo de prevenção e de mitigação de incidentes cada vez mais difícil e sofisticado.

Não são apenas as ameaças externas que representam riscos a uma corporação. Os próprios funcionários representam alto risco quando mal-intencionados ou mesmo quando não conscientes dos riscos envolvidos na manipulação da informação.

A norma ISO/IEC 27002:2005, é um padrão reconhecido internacionalmente na área da segurança da informação, amplamente utilizada para esboçar políticas de segurança, com o objetivo de proporcionar uma base comum para o desenvolvimento de um padrão organizacional e uma prática efetiva na gestão da segurança da informação.

Surge, então, um desafio adicional na gestão da segurança SI de uma organização: Qual é o nível da segurança dos SI da Inpharma?

Justificação do Tema

Um conjunto de controlos por si só não garantirá uma solução completa de segurança, o mesmo deve ser implementado com outras práticas e modelos adotados na área de TI para apoiar as metas da organização.

Segundo a norma NBR ISO/IEC 27002 (ABNT, 2005), a segurança da informação deve preservar os critérios de disponibilidade, integridade, confidencialidade, autenticidade, responsabilidade, não-repúdio e confiabilidade. A mesma preconiza:

As organizações, seus sistemas de informação e redes de computadores são expostos a diversos tipos de ameaças à segurança da informação, incluindo fraudes eletrônicas, espionagem, sabotagem, vandalismo, incêndio e inundação.

Portanto, a escolha do tema surgiu do interesse de utilizar a norma ABNT NBR ISO/IEC 27002:2005 para detetar as vulnerabilidades no Sistema de Informação da Inpharma por meio de uma análise baseada nas melhores práticas do mercado, orientado pela norma.

A escolha do tema também surgiu do interesse em confrontar a teoria existente com a realidade observada no contexto da Segurança de Sistema de Informação da Inpharma.

Objetivo Geral

Analisar a segurança do Sistema de Informação da Inpharma, baseada nas melhores práticas do mercado, orientado pela norma ISO/IEC27002:2005.

Objetivos Específicos

Para facilitar a compreensão do objetivo geral, entendeu-se decompô-los nos seguintes objetivos específicos:

- Compreender as noções básicas de Segurança dos Sistemas de Informação e os diferentes aspetos relacionados com as mesmas;
- Analisar as principais vulnerabilidades de Segurança Sistema de Informação da Inpharma, baseada nas melhores práticas do mercado, orientado pela norma ISO/IEC27002:2005;
- Propor ações para minimizar as vulnerabilidades encontradas, no contexto do plano de Segurança do Sistema de Informação.

Metodologia

Em relação á metodologia adotada, o trabalho foi elaborado com base em pesquisas bibliográficas, nomeadamente consultas de livros, trabalhos científicos já divulgados, e pesquisas em sites académicos.

Através da aplicação deste trabalho foi possível a entrevista com o Administrador de Sistema de Informação da Inpharma, como também com a Responsável pelo Gabinete de Administração e de Recursos Humanos.

Para além disso foi possível fazer a observação direta da infraestrutura com o objetivo de conhecer e interpretar a realidade direta da Segurança do SI nesta instituição, entre troca de ideias com técnicos do sistema de informação da Inpharma, como também de outras pessoas com conhecimento na área de estudo, procurando sempre não perder a coerência e consistência da informação.

Estrutura do trabalho

O presente trabalho encontra-se estruturado da seguinte forma:

- **Introdução/Contextualização** – nessa parte apresenta-se a contextualização do trabalho tendo o objetivo geral, os objetivos específicos, a metodologia utilizada e a composição do trabalho.
- **Capítulo 1: Segurança do Sistema de Informação** – nessa seção aborda-se a fundamentação teórica da Segurança do Sistema de Informação, mostrando a sua a definição do conceito, ameaças, análise do risco, áreas de segurança, testes e auditorias e ainda a segurança face ao desastre.
- **Capítulo 2: Plano Global de Segurança** – neste capítulo são abordados alguns aspetos relativos ao plano global de segurança, tais como plano de reposição, contingência como também outros documentos de segurança tais como a política de segurança, normas de segurança e ainda os procedimentos.
- **Capítulo 3: O Caso INPHARMA** – nessa apresenta-se o estudo de caso da Segurança dos Sistemas de Informação da Inpharma, onde são abordados diversos aspetos, tais como, a história, visão, missão e valores, a arquitetura de rede, as medidas de segurança, os resultados, seguido da conclusão.

Capítulo 1: Segurança dos Sistema de Informação

Antes de abordar a temática da Segurança dos Sistema de Informação é de extrema importância que se conheça alguns conceitos chave relacionados com a Segurança. E um dos conceitos que necessita ser bem compreendido, é o da Segurança, visto que é um fator decisivo na gestão das organizações, por ser um recurso importante e indispensável tanto no contexto interno como também no externo.

1 Conceito de Segurança do Sistema de Informação

A perceção do conceito de Sistemas de Informação (SI) dentro de uma organização é de extrema importância para o processo da Segurança dos Sistemas de Informação (SSI), de forma a recolher informações precisas que melhor auxiliam nessa tarefa.

Embora não exista uma definição universalmente aceite sobre o conceito da Segurança do SI, muitos autores abordam esses conceitos mostrando a forte relação entre a organização, a segurança e a informação.

No entender da IOT (2002) segurança é tida como “a tentativa de minimizar a vulnerabilidade de valores e recursos, entende-se, neste domínio, por vulnerabilidade o atributo de qualquer situação a partir da qual terceiros podem penetrar num SI informatizado sem qualquer autorização no sentido de tirar proveito do seu conteúdo ou das suas características, nomeadamente configuração e alcance”.

Mas para Oliveira (2000), a segurança é "(...) a restrição dos recursos de um microcomputador, ou de uma rede, onde porções desta rede para outros utilizadores ou computadores. Segurança não é mais do que a gestão de tal restrição”.

A segurança da informação é a proteção da informação contra vários tipos de ameaças de forma a assegurar a continuidade do negócio, minimizando danos comerciais e maximizando o retorno sobre investimentos e oportunidades de negócios (ABNT, 2005).

Para Carneiro (2002), a segurança dos sistemas de informação define-se como, “um conjunto de medidas e procedimentos, que têm por finalidade evitar que a informação seja destruída, alterada ou acedida, incidental ou intencionalmente, de uma forma não autorizada”.

De acordo com Simões (2004):

"A segurança de um sistema de informação pode ser entendida como um conjunto de medidas que visam a proteção desse sistema contra ameaças que afetem a confidencialidade, integridade e disponibilidade da informação processada”.

Beal (2005) afirma que a Segurança da Informação consiste em garantir que a informação existente em qualquer formato está protegida contra o acesso por pessoas não autorizadas (confidencialidade), está sempre disponível quando necessária (disponibilidade), é confiável (integridade) e autêntica (autenticidade). Estes conceitos são vistos como suporte para a Segurança da Informação.

Nesse sentido, podemos definir a segurança dos SI como um conjunto de medidas e procedimentos, que têm por finalidade evitar que a informação seja destruída, alterada, ou acedida, incidental ou intencionalmente, de uma forma não autorizada.

2 Ameaças

Ameaça é uma “causa potencial de um incidente indesejado, que pode resultar em um dano para um sistema ou organização”(IMA, 2014)¹.

A ameaça pode ser definida como sendo um evento com um impacto indesejado que pode resultar na perda, dano, divulgação de um ativo organizacional.

Para a CNASI (2012)², as ameaças à segurança de uma organização estão sempre, relacionados com a perda de uma (ou mais) das suas três características principais que são:

1. Perda da **Integridade**, acontece quando certa informação fica exposta ao manuseio de uma pessoa não autorizada, que acaba por efetuar alterações não aprovadas e sem o controle, privado ou corporativo do proprietário da informação;
2. Perda da **Confidencialidade**, ocorre quando há uma quebra de sigilo de uma determinada informação, como a senha de um utilizador ou administrador, por exemplo, que permite com que informações restritas, que deveriam estar acessíveis, apenas, para um determinado grupo de usuários, fiquem expostas;
3. Perda da **Disponibilidade**, acontece quando a informação deixa de estar acessível, justamente, por quem necessita dela. É o caso que ocorre com a perda de comunicação com um sistema importante para a empresa, que pode acontecer com a queda de um

¹ Disponível em <http://www.ima.sp.gov.br/politica-de-seguranca-da-informacao/> Consultado em 19 de Junho de 2014.

² Congresso de Segurança da Informação, Auditoria e Govenança da TIC

servidor, de uma aplicação crítica de negócio, que pode apresentar uma falha, devido há um erro causado por motivo interno ou externo ao equipamento³.

A segurança de sistemas de informação é caracterizada pela preservação dos três atributos básicos da informação: disponibilidade, confidencialidade, integridade e privacidade no acesso aos dados e funcionalidades dos SI (ABNT, 2005). Na dinâmica do seu armazenamento, processamento e transmissão as informações armazenadas podem sofrer vários tipos de ameaças⁴:

- Intrusos – utilizadores não autorizados a aceder ou modificar informação.
- Utilizadores autorizados maliciosos – utilizadores autorizados a utilizar o sistema, aproveitam para praticar atos ilícitos e atuam como intrusos, acedendo ou modificando dados de uma forma ilícita.
- Utilizadores autorizados e negligentes – utilizadores autorizados a acederem à informação que de uma forma não deliberada realizam certas ações que levam à modificação da informação ou permite que pessoas não autorizadas o façam.

De acordo com o resultado que podem produzir, essas ameaças podem ser classificadas:

- Rejeição;
- Revelação;
- Modificação;
- Falsificação.

Cada uma dessas ameaças possui formas específicas de atuar sobre os dados nos servidores, clientes. Os itens seguintes, analisam sinteticamente essas ameaças:

³ Disponível em <http://www.cnasi.com.br/ameacas-a-seguranca-da-informacao-de-uma-corporacao/> Consultado em 20 de Abril de 2014

a) Rejeição

Quando o autor de um determinado documento refuta a autoria do mesmo ou um utilizador nega ter enviado determinada informação apesar de efetivamente o ter feito, está-se perante um caso de rejeição.

b) Revelação

Segundo Mamede (2006) “por confidencialidade entende-se o manter seguro o conteúdo de uma mensagem evitando que possa ser acedido por alguém não autorizado para o fazer, tornando-se dessa forma conhecedor do mesmo”.

Conforme Rosa (2004),”pode ocorrer perda de confidencialidade e privacidade, quando os dados estiverem armazenados em servidores, clientes ou mesmo quando estiverem em trânsito. No caso dos servidores, o atacante procura ganhar acesso através da exploração de eventuais falhas como mecanismos de controlo de acesso inadequados, erros de programação, etc. Utilizadores autorizados podem igualmente revelar informações aos não autorizados. Do lado dos clientes, os dados estão sujeitos à revelação, quando por exemplo estiverem em sistemas operativos inseguros, ou executarem aplicações obtidas na Internet.

Quando em trânsito, os dados podem ser observados através de roteamento erróneo escutas telefónicas etc. Aplicações e redes não protegidas, são vulneráveis a todo tipo de ameaças. Contudo, quando estiverem convenientemente protegidas, estão apenas sujeitos às ameaças de utilizadores autorizados”.

c) Modificação

Segundo Mamede (2006) a integridade pode ser entendida como “ (...) a deteção de alterações como sejam adições ao conteúdo, eliminação parcial ou qualquer outra modificação

⁴ Disponível <http://bdigital.unipiaget.cv:8080/jspui/handle/10964/241/> Consultado em 20 de Abril de 2014

por pessoas não autorizadas a fazê-lo”. Como pode-se entender, a integridade permite evitar a modificação de dados por pessoas não autorizados.

Silva, Carvalho, e Torres (2003), afirmam que qualquer que seja a modificação ou erro que ocorra sobre os dados originais, a mensagem deixa de ser íntegra, podendo comprometer um enorme volume de dados, acarretando elevados prejuízos.

d) Falsificação

Monteiro, e Boavida (2000), definem a autenticidade como “ (...) o processo através do qual é validada a identidade de um utilizador, dispositivo ou processo”.

A autenticação pode ocorrer quando se falsificam os dados armazenados nos servidores; quando se criam servidores fantasma ou quando se alteram a origem dos dados que são apresentados ao servidor, tanto ao nível de utilizador como de servidor de origem. De acordo com (Medeiros, 2001) o serviço de autenticação pode ser implementado por mecanismos de *password* ou assinatura digital, estas questões serão desenvolvidas nos próximos pontos deste capítulo.

Existem várias outras ameaças relacionadas com o próprio ambiente envolvente incluindo portanto desastres naturais, falhas elétricas, estragos físicos acidentais e ataques físicos.

Conforme a norma (ABNT, 2008), as ameaças podem ser classificadas em três grupos:

- a) Ameaças naturais – estão ligadas aos fenómenos da natureza e qualquer organização está exposta a isso, são exemplos: as inundações, incêndios, furacões e tornados;
- b) Ameaças intencionais – são ameaças que são criadas com a intenção de prejudicar, causar dano, por exemplo, fraudes, sabotagem, roubo;
- c) Ameaças involuntárias – são ameaças que acontecem por falta de conhecimento e preparo dos usuários. Exemplos: propagação de vírus e spam.

3 Análise de Risco

Uma análise de risco define-se como sendo um processo de avaliar em que medida é que um determinado contexto que inclui ameaças, vulnerabilidades e o valor a proteger, é ou não aceitável para uma organização.

Segundo Carneiro (2002) uma análise de risco é muito mais do que avaliar a possibilidade de ocorrerem eventos negativos. Interessa fazer uma avaliação económica do impacto destes eventos. Esse valor poderá ser utilizado para comparar com o custo da proteção da informação em análise. Além disso, é necessário analisar a probabilidade de ocorrência dessas situações e considerá-las na elaboração de um plano de ação adequado.

A análise de risco inclui a aproximação sistemática de estimar a dimensão e impacto de riscos inerentes à segurança da informação na organização, assim como o processo de comparação entre os riscos estimados face ao critério de determinação do impacto dos mesmos na organização. Ela é um dos aspetos chave da norma ISO/IEC 27001, uma avaliação dos riscos é uma das exigências desta norma. Como resultado da avaliação de riscos, deve ser feita uma lista dos riscos identificados, classificados em ordem de gravidade para posteriormente serem tomadas medidas.

Segundo a norma (ABNT, 2005) a avaliação dos riscos identificados no campo da segurança da informação, deverá ter um alcance claramente definido, com o objetivo de ser eficaz. Se apropriado deverá conter a avaliação dos riscos de outras áreas da organização.

A avaliação dos riscos deve ser feita tendo em conta uma análise de custo-benefício, para revelar se compensa um risco ser minimizado ou transferido. Em suma, se um risco tem baixa probabilidade de ocorrer e o seu custo de tratamento é elevado, não compensa essa tomada de decisão.

Os requisitos de segurança são identificados através de uma avaliação sistemática dos riscos de segurança. Os investimentos na implementação dos controles de segurança, deverão ser analisados de acordo com os danos causados ao negócio da organização, que poderão ser gerados pelas potenciais falhas na segurança.

Segundo Carneiro (2002), logo que seja elaborada uma lista dos fatores de risco existentes, pode-se organizar uma tabela que mostra o grau de risco de cada uma deles, como a que se apresenta a seguir:

Tipo de Fator de Risco	Grau de Risco
Roubo de hardware	Baixo
Vandalismo	Medio
Deficiência nos equipamentos	Medio
Fraude	Baixo
Fogo	Muito baixo
Vírus Informáticos	Medio
Erros humanos	Medio
Acessos não autorizados	Medio
Roubo de informação	Medio

Tabela 1: Fatores e grau de risco, adaptado (Carneiro, 2002)

Segundo esta tabela, poderão ser tomadas as medidas pertinentes de segurança para cada caso em particular, tendo em atenção os custos previstos de acordo com o fator de risco apresentado (Caneiro,2002).

Depois de se ter definido o grau de risco, é necessário elaborar uma lista das medidas preventivas que devem ser tomadas e das correções a efetuar em caso de desastre. Esta lista deve ser ordenada de acordo com as prioridades e com as respetivas importâncias relativas.

É igualmente importante determinar a probabilidade da concretização das ameaças à segurança do sistema de informação. Essas informações deverão constar de um documento de análise de risco no qual os riscos são identificados, classificados, sendo depois especificado um conjunto de medidas a serem tomadas para se garantir a segurança. Nessa análise de risco, a segurança do sistema de informação é realizada em 4 etapas (Silva, Carvalho e Torres,2003):

I. Identificação de risco

A identificação dos riscos é conseguida através do levantamento do contexto de risco em que a organização se insere. Para se fazer essa contextualização, diversos modelos poderão ser empregues entre os quais se destacam a análise de SWOT⁵. Depois da contextualização, inicia-se então a identificação dos elementos necessários a análise de risco: As ameaças, as vulnerabilidades e os bens que poderão estar em perigo.

As ameaças podem ser identificadas tanto através da produção de diversos cenários como através da criação listas tipificadas concretizadas em árvores nas quais os ramos correspondem aos tipos de ameaças e as folhas correspondem às ameaças propriamente ditas.

Para que se possa fazer o cálculo probabilístico da concretização das ameaças identificadas, é importante fazer-se a identificação das vulnerabilidades. Á semelhança do que se verifica no processo de levantamento das ameaças, a identificação das vulnerabilidades pode ser efetuada através de árvores tipológicas em que os ramos correspondem aos tipos de vulnerabilidades e as folhas correspondem às vulnerabilidades propriamente ditas.

A identificação dos bens é necessária na análise quantitativa de risco, em que o mesmo é medido pelo impacto.

II. Análise de risco e impacto

⁵ Pontos fortes, pontos fracos, oportunidades e ameaças

Após a identificação das ameaças, vulnerabilidades e bens, pode passar-se à fase da caracterização dos riscos pela quantificação ou qualificação da probabilidade das ameaças gerarem danos. Deve-se igualmente efetuar uma análise sobre o impacto no negócio, identificando as atividades críticas para a sobrevivência da empresa em caso de desastre. Esta análise poderá servir igualmente para a criação do plano de continuidade de negócio face a desastres.

III. Identificação de controlos

A definição das medidas que deverão ser implementadas para aumentar a segurança do sistema de informação, deverá ser feita após o levantamento da situação organizacional em termos de risco. Portanto, o passo seguinte na análise de risco e de impacto, deverá ser a identificação e seleção dos mecanismos que permitem reduzir o efeito da ameaça ou danos decorrentes da sua concretização. A identificação dos controlos passa necessariamente pela definição de uma arquitetura para a segurança do sistema de informação assente numa estratégia global, contribuindo assim para o aumento da maturidade da segurança do SI.

A identificação de controlo deverá ainda levar em consideração uma abordagem específica para o controlo de riscos. Uma possibilidade é por exemplo a ordenação dos riscos por prioridade e correspondente identificação do controlo adequado para cada um.

IV. Analise dos controlos

Uma vez conhecida a situação da Empresa em termos de riscos, é chegado o momento de definir as medidas que deverão ser postas em prática para aumentar a sua segurança. O passo seguinte à identificação é a análise dos controlos, ou seja, dos processos ou dispositivos que permitam reduzir o efeito da ameaça ou os danos decorrentes da sua concretização.

Segundo Silva, Carvalho e Torres (2003) a seleção do tipo de controlo apropriado ao tratamento dos diversos riscos que ameaçam a Empresa pode ser auxiliada pela produção de um mapa de riscos, ou seja, pela representação dos riscos num gráfico bidimensional em função da sua frequência de concretização (num dos eixos) e impacto (no outro eixo).

A partir do mapa de risco assim criado, será possível implementar uma estratégia para a segurança, ordenando os riscos por prioridade e identificando o controle adequado a cada um, pela aplicação de regras baseadas nas áreas do mapa.

Exemplo: na figura 1 são representadas duas estratégias distintas, baseadas em mapas de risco.

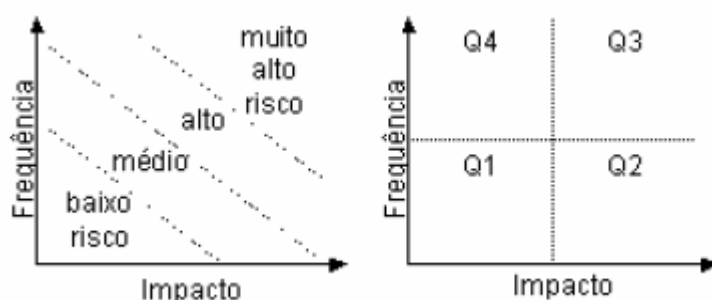


Figura 1: Regras Baseadas no Mapa de risco

Fonte: Silva, Carvalho e Torres (2003)

A estratégia indicada no mapa do lado esquerdo corresponde à prioridade conferida aos controles pela área correspondente ao grau de risco (de muito alto até baixo risco). A estratégia representada no mapa do lado direito define uma abordagem ao risco (evasão, redução, aceitação ou transferência) em função do quadrante do mapa em que este se encontre:

- Q1 - Aceitação;
- Q2 - Transferência (por exemplo, seguro);
- Q3 - Redução (da frequência e impacto do risco);
- Q4 - Evasão (redução da frequência de concretização do risco).

3.1 Sistema de Gestão de Risco

A norma NBR ISO/IEC 27005 (ABNT, 2008) propõe um modelo de Sistema de Gestão de Riscos da Segurança da Informação - SGRSI - que pode ser aplicado a qualquer tipo de organização. As etapas formam um ciclo que visa a melhoria contínua do SGRSI, conforme demonstra a figura 2.

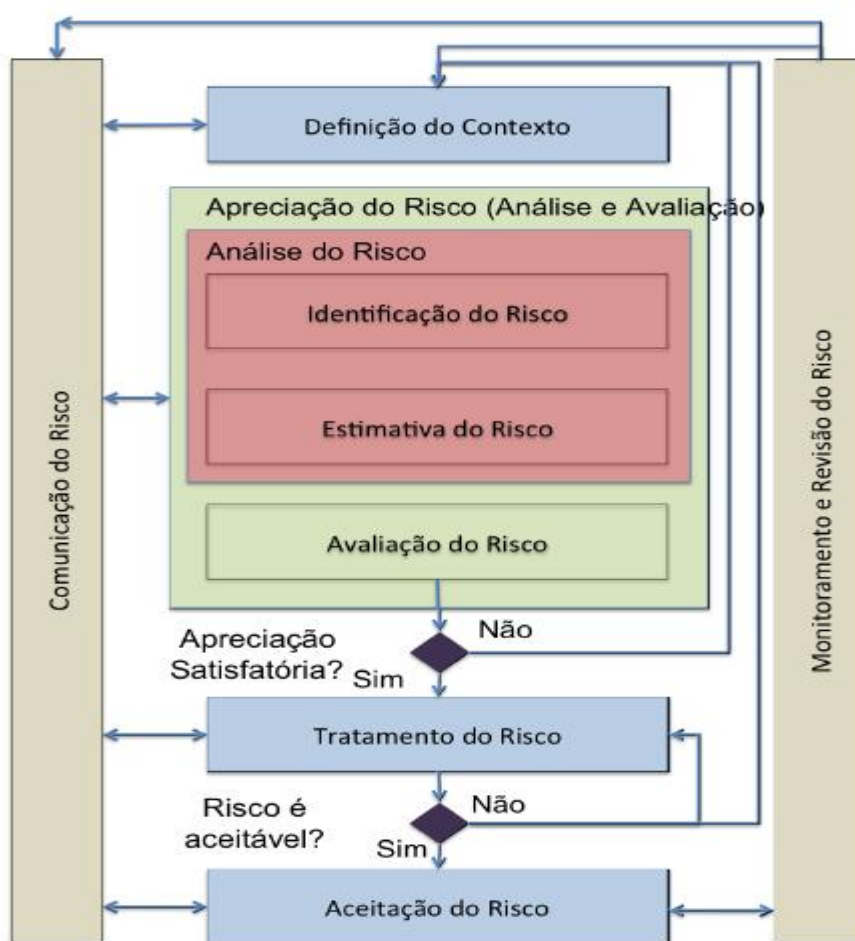


Figura 2: Etapas do Sistema de Gestão de Riscos da Segurança da Informação

Fonte: ABNT (2008)

As etapas do gerenciamento de riscos mostradas na figura 2 são tratadas abaixo, de acordo com a NBR ISO/IEC 27005 (ABNT, 2008):

➤ **Definição do Contexto**

Nesta etapa do modelo, é realizado o levantamento do contexto em que a organização está inserida, fatores internos e externos que podem afetar a política a ser adotada. As variáveis levantadas nesta etapa possibilitam a definição de requisitos e estratégias a serem adotados para o restante do processo.

É também nesta etapa que se define o nível aceitável de riscos dentro da organização, quais ativos serão considerados e como operar a gestão de riscos no órgão.

➤ **Apreciação dos Riscos**

Após a definição do contexto organizacional e da identificação dos critérios a serem adotados na Gestão de Riscos, a etapa de apreciação de riscos pretende analisar (quantitativa e qualitativamente) e avaliar o risco:

➤ **Análise do Risco**

A análise do risco é dividida nas etapas de 'identificação do risco' e 'estimativa do risco':

➤ **Identificação do Risco**

A identificação do risco visa verificar os fatores diretamente relacionados a ele, tais como o ativo, as ameaças, os controles, as vulnerabilidades e consequência:

➤ **Identificação de Ativos**

É necessário identificar os ativos da organização, com nível de detalhes suficiente para uma futura avaliação. Nesta etapa, também são mapeadas algumas características destes ativos, como funções, localização e responsáveis.

➤ **Identificação de Ameaças**

Neste momento, faz-se o mapeamento das ameaças inerentes a cada um dos ativos estudados na etapa anterior, juntamente com suas fontes (internas e externas) e suas especificidades (quanto à origem e ao tipo).

➤ **Identificação dos controles existentes**

Para cada risco, há uma forma de evitá-lo. Porém, controles ineficientes podem causar mais vulnerabilidades, aumentando a tendência ao risco.

Por isso, os controles devem ser mapeados e testados, a fim de identificar sua efetividade. Após a identificação do controle, deve-se planejá-lo.

Ressalta-se que um mesmo controle pode ser aplicado para diferentes riscos.

➤ **Identificação de vulnerabilidade**

É necessário mapear e monitorar as vulnerabilidades dos ativos da organização e respectivos controles, principalmente em ambientes de constantes mudanças.

➤ **Identificação de consequências**

Na possível atuação de um risco, que perdas nos objetivos da segurança (integridade, confidencialidade e disponibilidade) podem ocorrer? É necessário analisar os impactos que um risco pode causar e não omitir as brechas de segurança que possam existir.

As consequências de um evento de segurança (principalmente em empresas privadas) fazem com que a curva de tendência à falência aumente, até sua perda total. Por isso, a estimativa destas consequências deve conter valores quantitativos e qualitativos.

Conforme já mencionado, o custo contribui, principalmente para a gestão estratégica da organização.

➤ **Estimativa do Risco**

Por meio de abordagens qualitativas e quantitativas, pode-se atribuir valores para a probabilidade de atuação do risco e seus impactos. Na etapa "Estimativa do Risco", devem ser analisadas as relações custo x benefício, a severidade de tratamento do risco e o potencial de perda que o impacto do risco pode trazer à organização.

➤ **Avaliação do Risco**

De acordo com a relevância para os objetivos de negócio da organização, podem avaliar-se os riscos em níveis de prioridades. Ou seja, as decisões consequentes da avaliação devem ser tomadas com os critérios estabelecidos na primeira etapa do processo de Gestão do Risco. Destaca-se que as definições do contexto devem ser revistas periodicamente.

➤ **Tratamento dos Riscos**

A análise e avaliação dos riscos resultam numa lista ordenada de riscos, de acordo com a sua prioridade. Esta lista serve de base ao tratamento do risco, que depende de uma decisão estratégica:

1. Redução do Risco - decisões que visam reduzir a probabilidade e as consequências negativas através da adoção de controlos e ações [ISO Guia 73 (ABNT, 2009)];
2. Retenção do Risco - "aceitação do ônus da perda ou do benefício do ganho associado a um determinado risco" [ISO Guia 73 (ABNT, 2009)];
3. Evitar o Risco - decisão tomada visando o não-envolvimento ou a retirada da situação de risco [ISO Guia 73 (ABNT, 2009)];
4. Transferência do Risco - "compartilhamento com outra entidade do ônus da perda ou do benefício do ganho associado a um risco." [ISO Guia 73 (ABNT, 2009)];

➤ **Aceitação dos Riscos**

A aceitação é a etapa em que há o registo formal devidamente justificado da aceitação dos riscos residuais existentes na organização, com a relação de responsabilidades dos gestores.

➤ **Comunicação**

Segurança é responsabilidade de todos da organização. Por isso, é importante que a comunicação esteja presente em todo o processo de gestão de riscos, para maior efetividade do SGRSI.

➤ **Monitoramento e Revisão**

Quaisquer mudanças no contexto da organização e no panorama de risco devem ser revisadas para manter os negócios da organização em conformidade com a gestão de riscos empregada. Alguns aspectos que devem ser frequentemente monitorados são:

- Novos ativos e seus valores;
- Novas ameaças internas e externas;
- Alteração na legislação interna à organização;
- Contexto de mercado;
- Possibilidade de novas ameaças explorarem novas vulnerabilidades;

“A organização deve estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão da Segurança da Informação (SGSI) documentado dentro do contexto das atividades de negócio globais da organização e os riscos que ela enfrenta.” (ABNT, 2006) Conforme a figura 3, o Planeamento, Execução, Controle e Ação (PDCA) é um modelo que irá criar, manter e aperfeiçoar o SGSI.

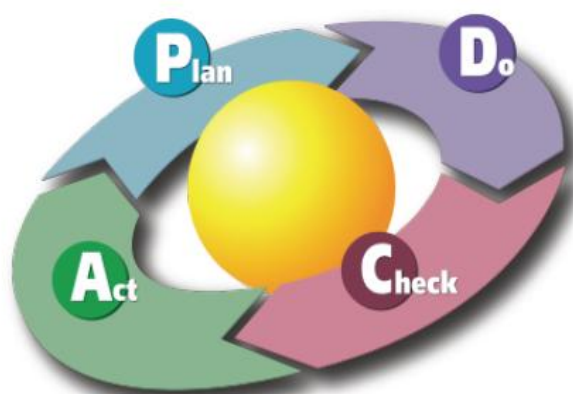


Figura 3: Modelo PDCA aplicado aos processos do SGSI

Fonte: ABNT (2006)

O processo de gestão de riscos é alinhado com o processo do sistema de gestão de segurança da informação de acordo com o padrão estabelecido na norma ISO 27001:2005, que adota o sistema PDCA.

A tabela 2 faz um resumo das atividades relevantes de gestão de riscos de segurança da informação para as quatro fases do processo do SGSI:

Processo do SGSI	Processo de gestão de riscos de segurança da informação
Plan - Planejar	Definição do contexto; Análise/avaliação de riscos; Plano de tratamento do risco; Aceitação do risco.
Do – Executar	Implementação do plano de tratamento do risco.
Check - Verificar	Monitoramento contínuo e análise crítica de riscos.
Act - Agir	Manter e melhorar o processo de Gestão de Riscos de Segurança da Informação.

Tabela 2: Alinhamento do processo do SGSI e do processo de gestão de riscos de segurança da informação, adaptado (ISO/IEC 27005:2008)

Em um SGSI, a definição do contexto, a análise/avaliação de riscos, o desenvolvimento do plano de tratamento do risco e a aceitação do risco, fazem parte da fase "planejar". Na fase "executar" do SGSI, as ações e controles necessários para reduzir os riscos para um nível aceitável são implementados de acordo com o plano de tratamento do risco. Na fase "verificar" do SGSI, os gestores determinarão a necessidade de revisão das avaliações e tratamento do risco à luz dos incidentes e mudanças nas circunstâncias. Na fase "agir", as ações necessárias são executadas, incluindo a reaplicação do processo de gestão de riscos de segurança da informação (ABNT, 2008).

4 Áreas da Segurança da Informação

Segundo Ferreira e Araujo (2006), o papel das áreas de segurança nos negócios tem-se tornado uma vantagem competitiva, pois embora alguns acreditem que adiciona burocracia, podemos considerar que os controlos aumentam de forma significativa a capacidade da organização para não estar tão exposta às perdas financeiras provenientes de fraudes, erros de processamentos, entre outras possibilidades.

Dizem que a função básica das áreas de Segurança da Informação "é proteger o ativo de informação, minimizando os riscos para níveis aceitáveis. Em algumas organizações, esta área também é responsável pela elaboração do plano de continuidade do negócio" (Ferreira e Araújo, 2006).

A segurança da Informação não envolve somente o ambiente de tecnologia, mas também envolve diversas áreas de segurança, que de seguida são apresentadas.

4.1 Segurança Física

O ambiente físico no qual a empresa opera, normalmente é tratado com uma certa indiferença, visto que muitas empresas não dão o devido valor a esta questão. A segurança física é o passo inicial para a defesa da corporação no sentido de proteger as suas informações contra acessos não autorizados.

A segurança em tecnologia da informação pode ser compreendida por dois principais aspetos: segurança lógica e segurança física. A segurança física desempenha um papel tão importante quanto a segurança lógica, porque é a base para a proteção de qualquer investimento feito por uma organização. Investir em diferentes aspetos da segurança sem observar suas devidas prioridades pode ocasionar uma perda de todos os recursos investidos em virtude de uma falha nos sistemas mais vulneráveis (Ferreira e Araújo, 2006).

Convém que sejam utilizados perímetros de segurança (barreiras tais como paredes, portões de entrada controlados por cartão ou balcões de receção com rececionistas) para proteger as áreas que contenham informações e instalações de processamento da informação (ABNT, 2005).

Segundo Carneiro (2002), o principal objetivo da segurança física é garantir a proteção dos SI quanto às suas dimensões físicas e no que se refere a todos os seus componentes nomeadamente hardware, software, documentação e meios magnéticos. Esta proteção relaciona-se com os riscos por perdas, extravios ou por danos físicos.

Interessa considerar a segurança física do SI tal como se apresenta na tabela seguinte:

Segurança Fica	Objetivos
Do pessoal	Reduzir os riscos devidos aos erros humanos, fraudes, roubos e a má utilização dos recursos existentes
Do equipamento	Proteger o hardware computacional, outros equipamentos, as suas interligações e o fornecimento de energia.
Das instalações	Requisitos da localização e estrutura dos edifícios destinados aos centros de informática de forma a garantir um nível de segurança adequado.

Tabela 3: Segurança Física, adaptado de (Carneiro, 2002).

Qualquer acesso às dependências da organização, desde áreas de trabalho até àquelas consideradas críticas (onde ocorre o processamento de informações críticas e confidenciais) deve ser controlado sempre fazendo necessária sua formalização (Ferreira e Araújo, 2006).

Segundo a (ABNT, 2005), convém que as áreas seguras sejam protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso.

De acordo com a mesma norma, as seguintes diretrizes para implementação devem ser levadas em consideração:

- A data e hora da entrada e saída de visitantes sejam registradas, e todos os visitantes sejam supervisionados, a não ser que o seu acesso tenha sido previamente aprovado; convém que as permissões de acesso sejam concedidas somente para finalidades específicas e autorizadas, e sejam emitidas com instruções sobre os requisitos de segurança da área e os procedimentos de emergência;
- Acesso às áreas em que são processadas ou armazenadas informações sensíveis seja controlado e restrito às pessoas autorizadas; convém que sejam utilizados controles de autenticação, por exemplo, cartão de controlo de acesso mais PIN, para autorizar e validar todos os acessos; deve ser mantido de forma segura um registro de todos os acessos para fins de auditoria;
- Seja exigido que todos os funcionários, fornecedores e terceiros, e todos os visitantes, tenham alguma forma visível de identificação, e eles devem avisar imediatamente o pessoal de segurança caso encontrem visitantes não acompanhados ou qualquer pessoa que não esteja usando uma identificação visível;
- Aos terceiros que realizam serviços de suporte, seja concedido acesso restrito às áreas seguras ou às instalações de processamento da informação sensível somente quando necessário, este acesso deve ser autorizado e monitorado;

- Os direitos de acesso a áreas seguras sejam revistos e atualizados em intervalos regulares, e revogados quando necessário.

De acordo com Carneiro (2002), a segurança física inclui pelo menos os seguintes componentes:

- Controlos de acesso;
- Serviços contra incêndios;
- Fornecimento de energia;
- Sistema de ar condicionado;
- Dispositivo para deteção de fugas/infiltrações de água;
- Pessoal de Segurança;
- Telecomunicações.

Nesse sentido, para evitar tais ameaças e garantir a segurança física devem ser considerados vários aspetos entre os quais: segurança do equipamento, a localização geográfica das instalações; controlos de acesso, que de seguida se apresentam.

4.1.1 Equipamentos

Os equipamentos informáticos "são um dos recursos que exigem maiores cuidados de segurança, visto que é nela que circulam os fluxos de dados e informações da organização" (Carneiro, 2002).

Para a ABNT (2005), o objetivo do item segurança de equipamentos é impedir perdas, danos, furto ou comprometimento de ativos e interrupção das atividades da organização.

De acordo com Carneiro (2002), atualmente, os equipamentos são altamente complexos e só algumas pessoas com formação técnica conhecem em pormenor a estrutura e a configuração técnica dos equipamentos, o que pode ser uma fonte de deterioração caso não forem tomadas medidas como, por exemplo:

- O acesso deve ser restringido ao pessoal (técnicos e utilizadores) que tenha uma formação básica, capaz de criar uma consciência profissional sobre o valor dos equipamentos enquanto ativo empresarial;
- Não deve ser permitida a entrada no SI de pessoas não autorizadas, nomeadamente na utilização de terminais;
- Também periodicamente deve ser monitorada o estado de conservação e de limpeza de todos os equipamentos das suas interligações.

Segundo a ABNT (2005), é importante que os equipamentos sejam colocados no local ou protegidos para reduzir os riscos de ameaças e perigos do meio ambiente, bem como as oportunidades de acesso não autorizado.

Mas podemos dizer que o fogo é uma das principais ameaças da segurança física dos SI, podendo destruir totalmente os arquivos de informação, ou os equipamentos informáticos. Para reduzir esses riscos Carneiro (2002), aponta alguns cuidados a ter:

- A temperatura não deve ultrapassar os 18° C e o limite da humidade não deve ir acima dos 65% para evitar a deterioração;
- O pessoal deve ser treinado no sentido de saber usar os extintores;
- Devem existir extintores em todas as instalações do Departamento da Informática, colocados em locais tecnicamente adequados, e sendo conveniente que os mesmos sejam experimentados;

Conforme a ABNT (2005), devem ser levadas em consideração as seguintes diretrizes para proteger os equipamentos:

- Os equipamentos sejam colocados no local, a fim de minimizar o acesso desnecessário às áreas de trabalho;
- As instalações de processamento da informação que manuseiam dados sensíveis devem ser posicionadas para que o ângulo de visão seja restrito, de modo a reduzir o risco de que as informações sejam vistas por pessoal não autorizado durante a sua utilização, e os locais de armazenagem devem ser protegidos, a fim de evitar o acesso não autorizado;

Segundo a norma ABNT (2005), os equipamentos devem ser protegidos contra falta de energia elétrica e outras interrupções causadas por falhas das utilidades. Nesse sentido, recomenda-se o uso de UPS para suportar as paradas e desligamento dos equipamentos ou para manter o funcionamento contínuo dos equipamentos que suportam operações críticas dos negócios.

4.1.2 Instalações

A localização de um centro de informática e a estrutura das instalações deve respeitar um conjunto de requisitos físicos e ambientais indispensáveis ao seu bom funcionamento.

Uma área de segurança pode ser um escritório fechado ou diversas salas dentro de um perímetro de segurança física, que podem estar fechadas ou podem conter armários fechados ou cofres. Convém que a seleção e o projeto de uma área de segurança levem em consideração as possibilidades de dano causado por inundações, explosões, manifestações civis e outras formas de desastres naturais ou causados pelo homem. Convém que também sejam levados em consideração as regulamentações e padrões de segurança. Também devem tratar qualquer ameaça originada em propriedades vizinhas, como por exemplo vazamento de água de outras áreas (Salgado, Bandeira e Silva, 2004).

Segundo a ABNT (2005), deve ser projetada e aplicada segurança física para escritórios, salas e instalações.

As seguintes diretrizes devem ser levadas em consideração para proteger escritórios, salas e instalações:

- Devem ser levados em conta os regulamentos e normas de saúde e segurança aplicáveis;
- As instalações-chave devem ser localizadas de maneira a evitar o acesso do público;
- Disporem de uma única entrada para o centro de dados;
- Estarem isoladas de calor e poeira;
- Ausência de interferências eletromagnéticas;
- Inexistência de acentuado nível de poluição atmosférica;
- As salas onde se instalam os equipamentos deverão ter teto falsos, para permitir a passagem dos cabos de energia e de ligação, bem como a instalação de condutas e saídas para o ar condicionado;
- Os edifícios sejam discretos e deem a menor indicação possível da sua finalidade, sem letreiros evidentes, fora ou dentro do edifício, que identifiquem a presença de atividades de processamento de informações, quando for aplicável.

4.2 Segurança do Pessoal

Na segurança do pessoal, o objetivo é garantir que todos os utilizadores conheçam as suas responsabilidades, e esteja aptos a desempenhar suas funções, além de reduzir o risco de roubo, fraude e mau uso de recursos. As responsabilidades de segurança devem ser definidas antes da contratação, com a descrição adequada do trabalho e suas condições. Todas as pessoas devem ser selecionados adequadamente, especialmente para trabalhos sensíveis com

acesso a informações. Todos os utilizadores devem assinar um acordo sobre suas funções e responsabilidades relacionadas com a segurança (ABNT, 2005).

Um documento formal com as políticas normas e procedimentos deverá ser divulgado de forma clara a todos os utilizadores. Como também deverão ser dados a conhecer a todos os utilizadores condutas especificando as boas práticas na utilização dos recursos disponíveis e estabelecendo balizas de comportamento às pessoas no que diz respeito a questões de segurança.

4.2.1 *Recrutamento e Mudança de Contratação*

Segundo a ABNT (2005), o principal objetivo durante o recrutamento é assegurar que todas as pessoas estejam conscientes das ameaças e preocupações relativas à segurança da informação, suas responsabilidades e obrigações, e estão preparados para apoiar na política de segurança da informação da organização durante os seus trabalhos normais, e para reduzir o risco de erro humano.

Para Mamede (2006), o processo de recrutamento do funcionário para uma organização exige um *background*, para que a organização não possa correr o risco de contratar pessoas com registo criminal informático ou atitudes incorretas. O autor defende ainda que quando é recrutado um novo funcionário para a organização deve estar definido o que tem de ser criado a nível de sistema para que este possa ter acesso aos equipamentos informáticos.

Antes do emprego as responsabilidades de segurança devem ser levados em conta no recrutamento de funcionários permanentes, contratados e agentes temporários (por exemplo, através de descrições de trabalho adequados, pré-triagem emprego.) e incluídos em contratos (por exemplo, os termos e condições de emprego e de outros acordos assinados sobre os papéis e responsabilidades de segurança⁶).

⁶ Disponível em <http://www.iso27001security.com/html/27002.html/>, Consultado em 10 de Junho de 2014.

Durante o emprego, os gestores devem garantir que todos os funcionários estejam cientes e motivados para cumprirem com as suas obrigações de segurança da informação. Um processo disciplinar formal é necessário para lidar com violações de segurança de informação (ABNT, 2005).

Como parte das suas obrigações contratuais, os funcionários, e outros terceiros devem concordar e assinar os termos e condições de sua contratação para o trabalho, os quais devem declarar as suas responsabilidade e da organização para a segurança da informação.

A direção deverá exigir a todos os utilizadores, que utilizem os recursos de acordo com o estabelecido nas políticas e procedimentos da organização.

Todos os funcionários, devem devolver todos os ativos da organização que estejam em sua posse após a cessação das suas atividades, do contrato ou acordo.

Os direitos de acesso de todos os utilizadores às informações e aos recursos de processamento da informação devem ser retirados após o encerramento de suas atividades, contratos ou acordos, ou devem ser ajustados após a mudança destas atividades (ABNT, 2005).

4.2.2 Sensibilização e Formação

De acordo com Silva, Carvalho e Torres, (2003), uma das formas de ajudar os utilizadores a adotar a segurança é a sensibilização, que pode ser feita tanto por campanhas de divulgação, como através de sessões de esclarecimentos e formação, mostrando-lhes as razões do que lhes é solicitado e a forma segura de realizar as suas atividades quotidianas como por exemplo, através da aplicação da política de secretaria limpa e da destruição sistemática em equipamento adequado, dos documentos sensíveis, em vez de os deitar no lixo.

Como afirma Mamede (2006) “ (...) a formação em segurança deve ser disponibilizada a todos os colaboradores que concebam, implementem ou efetuem a manutenção de sistemas de

rede, bem como a todos os colaboradores da organização, sensibilizando-os para os variados problemas”.

O objetivo da formação segundo Ferreira, e Alves (1995) é “garantir que os utilizadores têm consciência das ameaças e preocupações respeitantes à segurança da informação e estão sensibilizados para apoiar a política de segurança da organização (...)”.

Em suma isto quer dizer que, a formação constitui prática importante na segurança do pessoal, de modo ao uso seguro das tecnologias de informação e comunicação, como também devem receber formação na correta utilização dos recursos das TI antes de lhes ser assegurado o acesso aos serviços das TI.

Ainda no âmbito da segurança do pessoal, Silva, Carvalho e Torres, (2003), defendem que deve-se evitar a atribuição a uma única pessoa de funções vitais para a organização, distribuindo preferencialmente para dois ou mais colaboradores.

Segundo a ABNT, (2005) todos os funcionários da organização devem receber treinamento apropriado em conscientização, e atualizações regulares nas políticas e procedimentos organizacionais relevantes para as suas funções.

Deve existir um processo disciplinar formal para os funcionários que tenham cometido uma violação da segurança da informação.

4.3 Segurança Logica

Esta é a área mais abrangente, requerendo, conseqüentemente, um estudo muito mais apurado e detalhado, visto que é indubitavelmente a área mais rica, mais complexa e mais difícil de gerir no que diz respeito à segurança dos sistemas de informação. Isso deve-se essencialmente ao ritmo acelerado da evolução tecnológica acompanhado pelo aumento da sua complexidade.

A segurança lógica baseia-se sobretudo, na gestão das autorizações de acesso aos recursos informáticos, baseadas na identificação e autenticação.

Devemos estar atentos aos mínimos detalhes que compõem este tipo de segurança visto que a informação é a principal ferramenta do processo decisório das empresas. Importa, pois, analisar diversos aspetos da segurança lógica que consistem na utilização de barreiras e na aplicação de procedimentos que controlam o acesso aos dados, de acordo com a concessão de prévias autorizações. Para garantir a segurança lógica, (Mamede, 2006) destaca vários aspetos a serem levados em consideração nomeadamente: autenticação e controlo de acesso; redundância, criptografia; antivírus; filtragem de conteúdos, deteção de intrusões, assinaturas digitais, os quais passa-se a fazer referência.

4.3.1 Autenticação e Controlo de Acesso

Conforme Silva, Carvalho e Torres (2003) a autenticação e o controlo de acesso "são quem assegura que nos somos quem dizemos ser e nos permite aceder aquilo a que temos direito, que a nível da infraestrutura (redes de comunicação), quer a nível aplicacional, através do fornecimento de credenciais do nosso conhecimento exclusivo". A autenticação e o controlo de acesso neste caso, garante que apenas os utilizadores autorizados tenham acesso aos recursos disponibilizados, o que constitui portanto, a base para o controlo de acesso aos recursos como também são elementos básicos para o processo de proteção da informação.

Os controlos de acesso lógico têm por objetivo segundo Mamede (2006):

“ (...) limitar o acesso a dispositivos como, por exemplo, impressoras, bem como a outros recursos e serviços, como sejam informação, aplicações e sistema, e ainda funcionalidades diversas”.

Por sua vez, Monteiro e Boavida (2000), afirmam que “as funções de autenticação estabelecem a identidade de utilizadores e/ou sistemas, tendo em vista a determinação das ações permitidas”. Eles fazem parte de um processo de dois passos que determina quem pode aceder determinado sistema. Durante a identificação o utilizador diz ao sistema quem ele é

(normalmente através de um nome de utilizador), e durante a autenticação a identidade é verificada através de uma credencial (uma senha, por exemplo) fornecida ao utilizador.

Este mecanismo permite controlar quais as pessoas autorizadas a entrar em determinado local e registar o dia e hora de acesso, controlando e decidindo as permissões que cada utilizador tem. Um sistema de controlo de acesso é constituído por diferentes equipamentos periféricos de controlo e comando, interligados a uma única unidade de controlo que permite, em diferentes pontos, vários acessos (ABNT, 2005).

4.3.2 Redundância

“A redundância pode ser obtida de várias formas, quer através de cópias manuais de dados, quer através de sistemas automatizados de proteção da informação. Na sua expressão mais complexa, estes mecanismos de proteção podem assumir a duplicação total da infraestrutura informática existente, numa localização remota, com transferência automatizada de dados entre locais. Este tipo de soluções, normalmente adotados para estruturas extremamente críticas e sem qualquer tolerância de *downtime*, implica um investimento inicial avultado e custos de manutenção que podem ser igualmente elevados”. (Silva, Carvalho e Torres, 2003): Por este motivo, as soluções mais comuns passam pela criação de *clusters* de máquinas e pela implementação de soluções de discos em RAID (em que a informação é partilhada por vários discos, sendo que a indisponibilidade de um deles não implica a indisponibilidade dos dados nele contidos).

Para Rosa (2004), no campo da proteção da informação, este mecanismo permite evitar a indisponibilidade da informação. Pode ser concretizado por exemplo através da utilização de RAID com paridade. O planeamento redundante das rotas de redes poderá ser um mecanismo muito útil na mitigação de ataques.

Ao nível da infraestrutura de suporte aos dados, existe a possibilidade de criar soluções redundantes a praticamente todos os níveis. Segundo Silva, Carvalho e Torres (2003), para além dos *clusters* de máquinas, já referidos, os próprios equipamentos ativos da rede de dados

(*router*, *switch*, *hub*, etc.) podem ser duplicados, criando estruturas redundantes, como se ilustra no exemplo da figura 4:

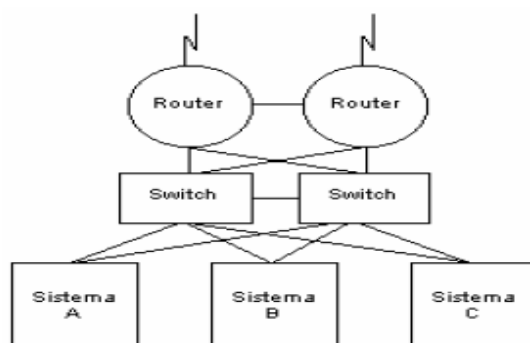


Figura 4: Infraestrutura redundante – Exemplo (Silva, Carvalho e Torres, 2003)

A proteção através da redundância encontra-se intimamente ligada com a questão do armazenamento.

4.3.3 Criptografia

Segundo Oliveira (2000), a criptografia é como “um conjunto de técnicas que tornam uma mensagem incompreensível permitindo apenas que o destinatário que conhece a chave de encriptação consiga descriptar e ler a mensagem com clareza”. O objetivo de criptografia, neste caso, é utilizar algoritmos de codificação e decodificação, para que o conteúdo da mensagem só pode ser decifrado pelo emissor e o recetor.

Para ABNT (2005), a criptografia é a arte de codificação que permite a transformação reversível da informação de forma a torná-la inteligível a terceiros. Esta utiliza determinados algoritmos numa chave secreta para, a partir de um conjunto de dados não criptografados, produzir uma sequência de dados criptografados.

Conforme Monteiro e Boavida (2000), distinguem duas categorias básicas de mecanismos de codificação: criptografia simétrica, também chamada de criptografia de chave secreta ou partilhada e criptografia assimétrica ou criptografia de chave pública.

4.3.3.1 *Criptografia Simétrica*

Na criptografia simétrica é utilizada uma única chave para cifrar e decifrar a mensagem. O emissor codifica a mensagem utilizando um algoritmo conhecido e uma chave secreta e envia, ao receber, o recetor descodifica a mensagem com a mesma chave secreta, conforme afirmam (Monteiro e Boavida, 2000). Nesse caso, segundo Mamede (2006), se a chave for quebrada num dos extremos toda a mensagem fica comprometida, e muitas vezes o outro extremo pode não se aperceber que a mensagem está comprometida. É recomendável que a mensagem e as chaves sejam transmitidas usando canais de comunicação diferentes.

Este mesmo autor (*idem, ibidem*) afirma que não obstante a sua velocidade que permite cifrar grandes quantidades de informação, apresenta como principal limitação o problema da gestão das chaves que pode ser desdobrada nos seguintes pontos:

- Se a chave é perdida, todo o canal fica comprometido;
- Convém mudar frequentemente de chave, para evitar o comprometimento da mesma;
- A distribuição das chaves é crítica, pois se houver algum comprometimento das chaves no momento em que as mesmas são distribuídas, todas as mensagens que utilizarem essas chaves podem ser decifradas por quem o interceptou;
- São necessárias várias chaves, aumentando o risco e a probabilidade da ocorrência de fuga de informação.

Conforme Moraes (2010), os algoritmos de chave simétrica, tanto o emissor como o recetor da mensagem devem possuir a mesma chave. Esses algoritmos são muito rápidos, mas existe problema de necessidade de um canal seguro para enviar a chave secreta, uma vez que existe o risco de a pessoa que descobrir a chave secreta conseguir decriptografar a mensagem.

A Figura 5 apresenta a criptografia simétrica ilustrando a chave única nas operações.

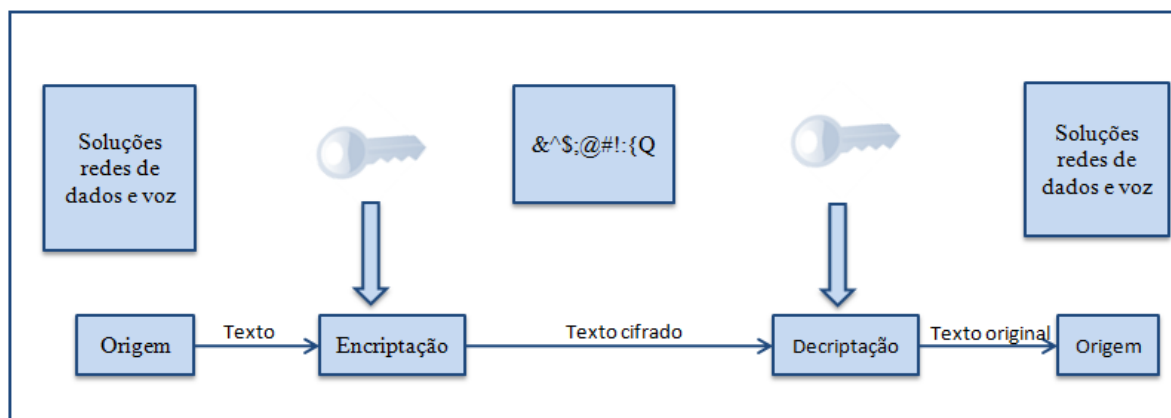


Figura 5: Criptografia Simétrica com uso de uma Única Chave, adaptado de (Moraes, 2010)

Os principais algoritmos de criptografia usados na criptografia simétrica são:

- RC2 (128 bits);
- 3DES;
- AES.

Para Mamede (2006) um dos algoritmos utilizados na criptografia simétrica é o DES. Para Silva, Carvalho e Torres, (2003) o DES é utilizado como *standard* para proteção da informação, desde 1981; surge depois o 3DES, composto por três operações sequenciais de cifra utilizando o DES, ou seja, para proporcionar maior segurança e aumentar o nível de proteção da informação, aplica o DES três vezes, utilizando chaves diferentes.

4.3.3.2 Criptografia Assimétrica

Conforme Moraes (2010), a Criptografia Assimétrica foi criado em 1976 por Whitfield Diffie e Martin Hellman, esse modo de criptografia baseia – se na utilização de duas chaves, sendo uma mantida secreta, enquanto outra pode ser divulgada publicamente.

Enquanto uma chave é utilizada para encriptação, outra é usada para deciptação. Esse modo, por ser mais complexo, é muito mais lento que a criptografia simétrica, algo de 100 a 1.000 vezes mais lento.

Se por um lado, a grande vantagem da criptografia assimétrica segundo Medeiros (2001), é que ultrapassado o problema de gestão das chaves, já não há necessidade de se ter um canal seguro para a transmissão da chave secreta, ou seja, o emissor não tem que dar ao recetor a conhecer secretamente a chave, porque a chave que cifra é diferente da que decifra a informação, tornando o processo mais seguro.

Por outro, Mamede (2006), afirma que “este tipo de criptografia é mais lenta que a criptografia simétrica, exigindo maior poder computacional”. Um outro problema ligado à utilização da criptografia assimétrica, segundo Silva, Carvalho e Torres, (2003) é que este tipo de criptografia não garante a autenticidade do remetente, ou seja, se a chave que cifra é a pública que pode ser trocada livremente, não há quaisquer garantias que a chave é a do destinatário pretendido. A autenticação, nesse caso, é garantida com recurso a assinatura digital, que de seguida passa-se a descrever.

A Figura 5 apresenta a criptografia assimétrica ilustrando a chave pública e privada nas operações.

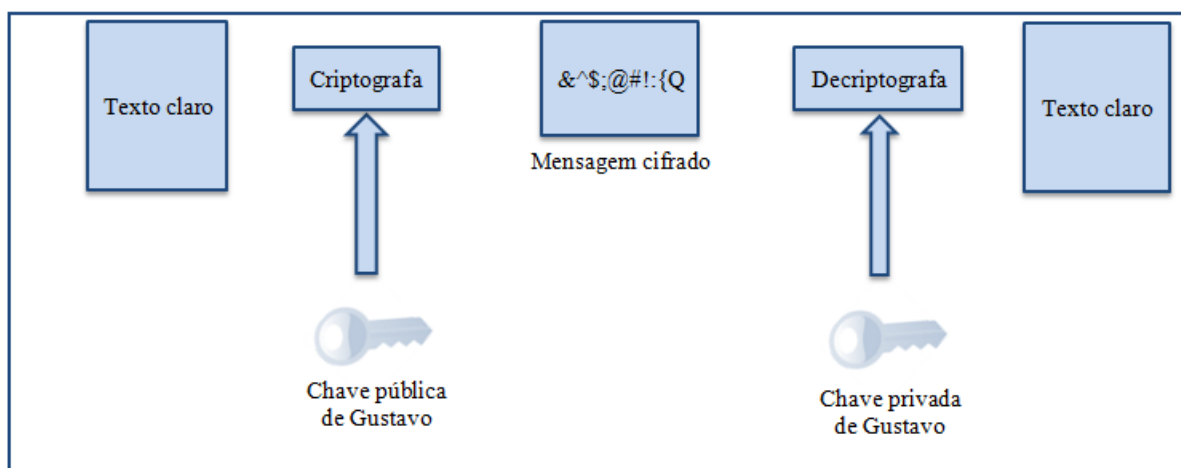


Figura 6: Criptografia Assimétrica, adaptado de (Moraes, 2010)

De acordo com Oliveira (2000), o algoritmo mais conhecido para a criptografia assimétrica é o RSA. Este algoritmo, de acordo com Medeiros (2001), pode ser usado tanto para criptografia de informações como para o sistema de assinatura digital.

4.3.4 Assinatura Digital

Este mecanismo é um conjunto de dados criptografados, associados a um documento que garantem a sua integridade e autenticidade. A utilização da assinatura digital prova que uma mensagem vem de um determinado emissor, porque é um processo que apenas o signatário pode realizar. No entanto, o recetor deve poder confirmar a assinatura feita pelo emissor e a mensagem não pode ser alterada, senão a assinatura não corresponderá mais ao documento. A validade de uma assinatura digital verifica-se se esta se baseia em certificados emitidos por entidades certificadas credenciadas.

Segundo ANAC (2014) a assinatura digital é um documento eletrónico que funciona como uma carteira de identidade virtual que permite a identificação segura do autor de uma mensagem ou transação feita nos meios virtuais, como a Internet⁷.

Funciona por meio de procedimento lógicos e matemáticos que asseguram a integridade das informações e a autoria das transações (ANAC, 2014).

Esse documento eletrónico é gerado e assinado por uma terceira parte confiável, ou seja, uma Entidade Certificadora, que no caso de Cabo Verde é assegurada pela Agência Nacional das Comunicações – ANAC, que, seguindo regras estabelecidas pelo Conselho Gestor da ICP-CV, associa uma entidade (pessoa, processo, servidor) a um par de chaves criptográficas.

A assinatura digital contém os dados de seu titular conforme detalhado na política de certificados de cada entidade certificadora fazendo com que o documento assinado digitalmente seja equivalente ao papel assinado de próprio punho.

O certificado digital para além de personificar o cidadão na internet garante a validade jurídica aos atos praticados com o seu uso.

⁷ Fonte http://www.anac.cv/index.php?option=com_content&view=article&id=143%3Anoticia-de-teste&catid=35%3Anoticias-banner&lang=pt, Consultado a 17 de Junho de 2014.

Trata-se de uma ferramenta que permite que aplicações como comércio eletrônico, assinatura de contratos, operações bancárias, iniciativas de governo eletrônico, entre outras, sejam realizadas com segurança (ANAC, 2014).

São transações feitas de forma virtual, ou seja, sem a presença física do interessado, mas que demanda identificação clara da pessoa que a está realizando pela internet⁸.

4.3.5 Antivírus

Nos dias de hoje com a proliferação de técnicas cada vez mais sofisticadas de código malicioso e com o aumento significativo de *hackers* e criminosos digitais espalhando *vírus*, *spam* e outras ameaças da internet, torna-se uma necessidade de qualquer organização que lida com os recursos das TI, dispor de mecanismos antivírus no seu sistema informático. Segundo Downing (2001), o antivírus é um “*software* que protege computador contra vírus (modificações destrutivas de *software*), impedindo as modificações que um vírus tente efetuar ou detetando, logo que seja possível um vírus que se introduza no computador”.

A atualização é igualmente um aspeto fundamental, independentemente das TI que se está a utilizar, o sistema antivírus deve estar configurado para fazer atualização automática. Normalmente os fornecedores de antivírus dispõem de paginas web que permitem fazer a atualização dos mesmos. Para Silva, Carvalho e Torres (2003), existem soluções centralizadas para realizar automaticamente e permanentemente a atualização e a disseminação dessas mesmas atualizações por todos os sistemas que se pretende proteger, a partir de um ponto único.

No entanto Mamede (2006), acrescenta ainda que “o sistema antivírus deverá estar instalado em cada servidor e em cada computador pessoal da organização”. Nesse sentido, é extremamente importante certificar-se de que este programa é atualizado pelo menos uma vez por semana, e que todos os drives sejam examinados constantemente.

4.3.6 Filtragem de Conteúdos

Os mecanismos de filtragem de conteúdos não se limitam em detetar mensagens em que os anexos podem conter algum código malicioso, mas desempenham outras funções especificamente em mensagens de correio eletrónico ou conteúdos *Web* e podem ser usados juntamente com o sistema antivírus.

Entre outras funções de filtragem de conteúdos podemos indicar a restrição a determinados acessos em termos de utilização da internet (como, por exemplo, cópia de filmes, acesso a conteúdos pornográficos, etc.); restringir o acesso a *software* ilegal, ou seja, definir o que é permitido e o que é negado aos utilizadores. É igualmente função deste mecanismo detetar e impedir tentativas de transmissão de informação confidencial de acordo com (Silva, Carvalho e Torres, 2003). Tais restrições podem ser feitas, de acordo com os mesmos autores (idem, ibidem) com base nas listas de endereços URL⁹, ou com base nas palavras-chave relacionadas com quaisquer temáticas que se pretende bloquear.

Silva, Alberto e Romao (2003) afirmam que muitas organizações “ (...) recorrem a esse tipo de serviços para garantir que os seus colaboradores não ocupam o seu tempo de trabalho a aceder a conteúdos que nada tem a ver com atividade profissional”. Por outras palavras, filtragem de conteúdos, contribui até para economizar recursos evitando o seu uso em práticas não relacionadas com atividades da instituição, o que resulta numa economia para a empresa em termos de recursos gastos para suportar atividades como por exemplo *downloads* ilegais.

4.3.7 Salvaguarda da Informação

Segundo Silva, Carvalho e Torres (2003) à medida que aumenta a capacidade de armazenamento disponível e cresce a complexidade dos sistemas de processamento de

⁸ Disponível em http://www.anac.cv/index.php?option=com_content&view=article&id=143%3Anoticia-de-teste&catid=35%3Anoticias-banner&lang=pt, Consultado em 17 de Junho de 2014.

⁹ URL (*Uniform Resource Locator*) é a forma única e exata de localizar a informação disponível na internet, Downing (2001).

informação, o volume de dados armazenados segue esta tendência, atingindo proporções significativas. As empresas, cada vez mais, deparam-se com a necessidade de proteção de um conjunto complexo de informação, disperso por vários suportes e gerado por diferentes aplicações. Felizmente, as soluções de salvaguarda, ou *backup*, atuais acompanharam esta evolução e oferecem hoje níveis de desempenho e de proteção amplamente satisfatórios.

Conforme Back (2013), a forma mais adotada para salvaguardar informações é a cópia de segurança.

Silva (1999) destaca que para se por em prática uma cópia de segurança, é preciso que a organização siga algumas etapas¹⁰:

➤ **Escolha dos dados**

Os arquivos que vão ser copiados devem possuir procedência confiável, ou seja, não serem infectados, pois quando a restauração for estabelecida, pode trazer uma série de problemas para o computador.

➤ **Mídia utilizada**

Há inúmeras formas para realizar um procedimento de cópia de segurança, a mesma pode ser efetuada por meios da utilização de CD, Blue Ray, HD, fitas magnéticas e entre outras variadas mídias que o backup pode ser realizado. A escolha de qual mídia vai ser utilizada, depende do que está sendo armazenada, a quantidade de informações que estão sendo armazenados, os níveis de confiabilidade que essa cópia deve possuir, ou seja, para a escolha de um dado para realizar a cópia de segurança é preciso que a camada de gestão defina o que pretendem armazenar.

➤ **Local de armazenamento**

¹⁰ Disponível em <<http://www.aedb.br/seget/artigos11/32614346.pdf>>, Consultado em 24 de Junho de 2014.

As cópias devem ser guardadas em um ambiente restrito e diferente do local que foi efetuado a cópia, por forma a diminuir as possibilidades de perdas de todos os dados em caso de desastre.

Segundo Back (2013) o processo de backup deve levar em conta as necessidades de recuperação de negócio e também questões legais do país onde o mesmo será executado além de questões de infraestrutura tecnológica que mantém grande parte das tarefas automatizadas funcionando.

Em empresas onde não há necessidades constantes de recuperação de informação em back-ups, é necessário a execução de testes de recuperação. Estes devem ser feitos com certa frequência a fim de manter sempre um bom índice de recuperação das informações.

Outro fator muito importante a ser considerado segundo o mesmo autor (idem) no processo de salvaguarda de informações é o armazenamento das fitas magnéticas ou de qualquer outro meio onde esteja sendo realizado a cópia de segurança. De nada adianta salvar informações em um dispositivo diferente do original se manteve-se o dispositivo junto ao original. Em caso de desastres, as vezes naturais, a perda da informação será total, incluído os dispositivos de armazenamento de back-ups. É deveras importante realizar o transporte seguro destes dispositivos para locais onde haja certa distância do ponto de origem além de segurança quanto ao próprio armazenamento em si.¹¹

Silva, Carvalho e Torres (2003), afirma que os esquemas de *backup* mais comuns enquadram-se na clássica definição de três ciclos: Avô, Pai e Filho. O que diferencia estas três “gerações” de *backup* é, precisamente, a duração do seu prazo de retenção e, eventualmente, o seu local de armazenamento.

¹¹ Disponível em <http://seginfoatual.blogspot.com/2013/12/a-importancia-dos-back-ups.html>. Consultado a 23de Maio 2014.

A cópia de segurança da geração “avô” é tipicamente a que mais tempo é retido, enquanto o “filho” constitui, normalmente, um *backup* de rotação rápida.

Exemplo:

- Cópia de segurança “avô”: *backup* completo dos sistemas, realizado na última sexta-feira de cada mês e retido durante trinta dias (ou mais).
- Cópia de segurança “pai”: *backup* completo dos sistemas, realizado todas as sextas-feiras, e retido durante quinze dias.
- Cópia de segurança “filho”: *backup* completo de todos os sistemas, realizado diariamente, e retido durante sete dias.

De acordo com Ribeiro (2009) há diversos métodos para realizar uma cópia secundária, dentre elas destacam-se¹²:

- **Cópia de segurança total**

O método de backup total tem a pretensão de copiar os documentos selecionados e armazená-los em um ambiente seguro, esse método é muito seguro e eficaz, no caso de uma cópia de segurança vier a dar problema, a cópia anterior a ela será restaurada, e assim futuramente diante caso a falha continue a persistir. No entanto esse modo de backup é muito lento e requer uma enorme capacidade de armazenamento, isso devido a cada backup que for realizado, o ultimo backup não será excluído.

- **Cópia de segurança incremental**

Consiste em um backup que registra somente os arquivos que foram modificados desde o último backup e irá acrescentá-los ao ultimo procedimento, esse tipo de backup requer uma

¹² Disponível em <<http://www.aedb.br/seget/artigos11/32614346.pdf>>, Consultado em 24 de Junho de 2014.

pequena quantidade de memória, contudo a sua restauração é a mais lenta dentre os modos transitados.

➤ **Cópia de segurança diferencial**

O modo de cópia de segurança diferencial tem como objetivo copiar os documentos inalterados do computador, o grande mérito desse método é que, a realização do backup é feita de forma rápida e eficiente, mas esse sistema é muito vulnerável a falhas, isso pode ser explicado caso a organização não tenham cópias dos arquivos inalterados, esse sistema de backup se tornará ineficaz.

Dependendo do prazo de retenção das cópias de segurança, deverá, então, ser delineado um esquema de armazenamento *onsite* e *off-site*, como forma de garantir a segurança e disponibilidade dos suportes.

A ABNT (2005), recomenda que o backup dos sistemas seja armazenado em outro local, o mais longe possível do ambiente atual, como em outro prédio. Nesse sentido a salvaguarda regular das informações armazenadas em meio seguro, é fulcral para a recuperação das funções da empresa em caso de falhas, como também definir o nível de criticidade e capacidade de cada ativo identificado.

Como boa prática de gestão, devem ser estabelecidas medidas alternativas de recuperação a desastres e continuidade de negócio para os ativos de maior criticidade para o negócio da Organização.

4.3.8 Detecção de Intrusões

De acordo com Silva, Carvalho e Torres (2003), os sistemas de detecção de intrusão oferecem visibilidade a uma organização das várias tentativas de intrusão, tanto no que sucede no seu exterior e mesmo ações internas de violação da segurança, como tentativas de acesso a recursos protegidos por parte de funcionários.

Segundo Santos (2010), existem diversas ferramentas que contribuem significativamente para melhoria da segurança de uma rede, tais como: a criptografia, que estabelece um nível de proteção para dados, o uso de Firewall estabelecem uma lógica na entrada e saída da rede controlando o tráfego a nível de pacotes, a VPN que cria um túnel criptografado entre 2 pontos de rede, etc...

Entre elas, o sistema de detecção de intrusão merece um destaque especial, pois engloba o processo de monitorar, identificar e notificar a ocorrência de atividades maliciosas, atividades não-autorizadas que coloquem em risco e tenham como alvo ativos de tecnologia de uma rede de computadores.

Os mesmos autores (idem, ibidem) dividem os sistemas de detecção de intrusão em dois grandes grupos, a seguir descritos¹³.

➤ **Sistemas de Detecção de Intrusão baseados em Host (HIDS)**

De acordo Santos (2010), o sistemas de Detecção de Intrusão baseados em Host monitora e analisa informações coletadas de um único Host (Máquina). Não observa o tráfego que passa pela rede, seu uso volta-se a verificação de informações relativas aos eventos e registros de logs e sistema de arquivos (permissão, alteração, etc.). São instalados em servidores para alertar e identificar ataques e tentativas de acesso indevido à própria máquina, sendo mais empregados nos casos em que a segurança está focada em informações contidas em um servidor e os utilizadores não precisam ser monitorados. Também é aplicada em redes onde a velocidade de transmissão é muito alta como em redes “Gigabit Ethernet” ou quando não se confia na segurança corporativa da rede em que o servidor está instalado.

➤ **Sistemas de Detecção de Intrusão baseados em Rede (NIDS)**

O Sistemas de Detecção de Intrusão baseados em Rede monitora e analisa todo o tráfego no segmento da rede. Consiste em um conjunto de sensores que trabalha detetando atividades

¹³ Disponível em <http://www.seginfo.com.br/sistemas-de-deteccao-de-intrusoes-ids-intrusion-detection-systems-usando-unicamente-sofwares-open-source/>. Consultado a 23de Maio de 2014

maliciosas na rede, como ataques baseados em serviço, portscans, etc... São instalados em máquinas responsáveis por identificar ataques direcionados a toda a rede, monitorando o conteúdo dos pacotes ou do tráfego e seus detalhes como informações de cabeçalhos e protocolos. Os NIDS têm como um dos objetivos principais detetar se alguém está tentando entrar no seu sistema ou se algum utilizador legítimo está fazendo mau uso do mesmo.

4.3.9 Resposta a ataques

Este ponto, não sendo exclusivo da segurança lógica, assume particular relevo neste campo, na medida em que é precisamente nesta área que o responsável pela segurança do SI da Empresa terá de tomar algumas decisões complexas.

Qualquer organização que possua sistemas informáticos ligados em rede está exposta a ataques, quer sejam oriundos de *script kiddies* (pessoas sem grandes conhecimentos técnicos, que se limitam a descarregar software de ataque da Internet e a utilizá-lo aleatoriamente contra alvos indiscriminados), quer sejam da autoria de inimigos determinados, equipados e organizados, decididos a provocar estragos avultados ou a roubar informação confidencial. O número de tentativas de infeção ou de tentativas de descoberta de vulnerabilidades de um sistema ligado à Internet ascende diariamente às várias centenas, ou mesmo milhares, dependendo do perfil do sistema em causa. Uma organização com bastante projeção na sociedade atrairá naturalmente mais atenções do que uma pequena Empresa praticamente desconhecida. Mas ninguém está isento desta realidade. Como tal, torna-se necessário prever o maior número possível de ocorrências, bem como a respetiva resposta. (Silva, Carvalho e Torres, 2003).

Hoje em dia, praticamente todos os sistemas informáticos fornecem uma qualquer forma de registar a utilização que deles é feita. Estes registos, ou *logs*, constituem os elementos que permitem reconstituir acontecimentos e ter uma visão da utilização que é dada a determinado sistema. Assiste-se, em muitos casos, à definição pouco cuidadosa do que fica registado, do respetivo grau de pormenor e do que fazer a esses registos. De facto, muitos são os sistemas

em que a definição de *logging* é rotativa, ou seja, ao fim de algum tempo, os registos mais recentes são sobrepostos a outros, mais antigos.

Deverá, pelo contrário, existir uma política de retenção de *logs* que defina não só a duração, volume e nível de detalhe desses registos, mas que estabeleça igualmente a sua remoção dos sistemas para locais seguros, ou para outros sistemas. Afinal, a última coisa que um atacante tipicamente faz, antes de deixar um sistema que acabou de penetrar, é eliminar o registo das suas atividades. Se este for copiado, em tempo real, para outro sistema informático da Empresa, a sua eliminação num sistema não impedirá ao responsável pela segurança a reconstituição dos eventos (Silva, Carvalho e Torres, 2003).

Com uma regularidade definida, esses registos deverão ser retirados dos sistemas e, por exemplo, copiados para um suporte digital, guardado em local seguro. Esta manutenção histórica poderá permitir, por exemplo, determinar o início das tarefas de exploração que conduziram a uma tentativa de intrusão. Ou poderão revelar a partir de quando é que um utilizador começou a imprimir documentação confidencial. Esta tarefa, que consome pouco tempo e recursos, poderá ser um meio valiosíssimo de determinação de acontecimentos e um precioso auxiliar na obtenção de provas incriminatórias contra um delinquente.

Porém, deve ser dada particular atenção à definição do que deve ser registado. Se, em certos sistemas, é conveniente registar toda e qualquer atividade, outros, por exemplo, apenas necessitarão do registo de entradas e saídas no sistema e de acesso aos ficheiros do sistema operativo. Esta definição, se não for cuidadosamente realizada, poderá criar uma quantidade de dados que, simplesmente devido ao seu elevado volume, se tornam impraticáveis de gerir.

Os registos são, efetivamente, a última arma na linha de defesa (e de reação) a ataques. São essenciais para determinar o que aconteceu, quando e como e são um instrumento fundamental na prossecução de ações punitivas.

Estas podem, e devem, ser equacionadas sempre que a organização considere haver lugar a retribuição pelos danos causados por um atacante, quer este seja um miúdo com tempo a mais nas mãos, quer se trate de um concorrente comercial.

É, portanto, essencial estabelecer normas e procedimentos claros e específicos que definem as linhas condutoras da organização. Não sendo possível prever todo o tipo de ataques que possam ocorrer, nem todas as formas de que estes se podem revestir, é fundamental que a organização saiba o que fazer.

A decisão deve ser tomada caso a caso, auxiliada por um procedimento, e fundamentada na realidade da ocorrência, sempre bem enquadrada nas linhas mestras da segurança empresarial, ou seja, no Plano de Segurança da Empresa.

Segundo Silva, Carvalho e Torres (2003) no caso da segurança física, a resposta a ataques encontra-se perfeitamente definida: no caso de um assalto, todos conhecemos bem os procedimentos a seguir, em resposta a esse acontecimento.

Qualquer organização que possui os seus recursos informáticos em rede está exposta a ataques. Nesse sentido, é importante definir as ações a serem levados a cabo em caso de ocorrência de ataques.

4.4 Testes e Auditorias

Atualmente assiste-se a uma oferta crescente de serviços de teste e de auditoria de segurança, cujo objetivo é o de avaliar o grau de proteção dos sistemas informáticos das organizações.

Independentemente da importância destas análises e da pertinência dos seus resultados, o responsável pela segurança informática deverá escolher cuidadosamente a altura adequada para a sua realização, dependendo dos objetivos que pretenda atingir. Conforme Silva, Carvalho e Torres (2003) analisaremos algumas possibilidades:

- Aquando da nomeação do responsável pela segurança: a Empresa contrata, ou nomeia, alguém para desempenhar as funções de responsável pela segurança. Uma das primeiras tarefas desse elemento poderá ser a de realizar uma análise de risco, ou contratar a terceiros uma auditoria de segurança, de modo a obter uma imagem, atual, do panorama de segurança da organização. Os resultados desta auditoria servirão de ponto de partida para a elaboração de soluções e para a correção das insuficiências detetadas.
- Após a implementação de medidas de segurança: Partindo do princípio de que o responsável pela segurança tem um conhecimento mais ou menos aprofundado da situação da Empresa, em termos de segurança lógica, este poderá tomar medidas preventivas e/ou corretivas, no âmbito do Plano Global de Segurança. Neste caso, os testes ou auditorias de segurança têm como objetivo avaliar a eficácia das medidas introduzidas e validar as decisões tomadas.
- Com regularidade temporal: Em paralelo ao desenvolvimento e implementação do Plano Global de Segurança, o responsável por esta poderá optar por um acompanhamento das medidas implementadas através de testes ou auditorias regulares à segurança. Poderá, deste modo, ter uma imagem mais real das consequências dos mecanismos adotados e adequar a introdução de novas soluções a estes resultados. Por outro lado, a obrigatoriedade deste tipo de auditorias regulares pode ser um requisito da própria organização.

Mas segundo o autor referido, (idem, ibidem) a decisão de realizar um teste ou uma auditoria aos sistemas, bem como a altura adequada para a sua execução, dependem das circunstâncias específicas da Empresa, bem como do orçamento disponível.

Segundo Rosa (2004), testes e auditorias aos sistemas de informação, são importantes para que se possa determinar o grau de proteção do sistema e determinar as ações a serem implementadas para aumentar os níveis de segurança. Deverão ser realizados regularmente. Contudo, é aconselhável a sua realização a título extraordinário, aquando da nomeação de um

novo responsável pela SSI¹⁴ ou após a implementação de novas medidas de segurança. Entre os aspetos que deverão ser considerados aquando da realização destes testes, destacam-se.

- **Auditoria completa dos sistemas** – análise exaustiva de todo sistema informático da instituição, tanto ao nível interno como externo (disponibilizados na Internet).
- **Testes de intrusão** – tentativas de acesso aos sistemas da empresa por parte de pessoas não autorizadas. Os resultados deverão entretanto ser úteis e não apenas descrições de ataques.
- **Teste de vulnerabilidades** – confronto dos sistemas e aplicações existentes com a lista das vulnerabilidades conhecidas. São normalmente realizadas por aplicações que possuem uma base de dados das vulnerabilidades existentes.
- **Engenharia Social** – consiste num conjunto simples de tentativas de obtenção de informação por exemplo através do telefone ou de ações mais complexas como tentativa de entrar nas instalações.

5 Segurança face ao desastre

“Um desastre consiste num acontecimento imprevisto que origina dificuldades e perdas à organização afetando significativa e de forma negativa a sua capacidade de executar serviços essenciais”. (Silva, Carvalho e Torres, 2003): Nem todos os incidentes resultam num desastre: a maioria provoca apenas um pequeno período de indisponibilidade, ou seja, uma emergência. Um desastre resulta de um incidente que afete a capacidade da organização em realizar as atividades de suporte aos seus processos críticos, durante um período superior ao limite máximo tolerado pelas funções do negócio. Ou seja, enquanto as funções da Empresa provocarem a paragem ou indisponibilidade de alguns processos de suporte, o incidente é considerado uma emergência. Este passará a desastre a partir da “declaração de desastre”, altura em que a organização assume inequivocamente a necessidade de ativação de medidas excecionais conducentes à recuperação dos processos e atividades afetados pelo incidente.

¹⁴ Segurança de Sistema de Informação

Em caso de desastre, segundo o mesmo autor o principal objetivo do negócio será, então, o de retomar todas as suas atividades críticas o mais rapidamente possível, o que acontecerá no período de recuperação. Só no final deste período serão retomadas as restantes atividades, não críticas, entrando a Empresa, assim, na fase de regresso à normalidade.

Para Silva, Carvalho e Torres (2003), como a probabilidade de ocorrência de desastres é algo real, torna-se necessário a definição de um plano de recuperação ou continuidade de negócio que visa garantir a recuperação das funcionalidades críticas da empresa de forma suficientemente rápida, de modo a garantir o não comprometimento da viabilidade institucional. Portanto esse planeamento visa identificar as atividades a serem realizadas em caso de desastres, os responsáveis pela sua excussão, os meios necessários e o modo de realização dessas atividades. Esse projeto é implementado em 5 fases:

1. Arranque;
2. Redução de riscos e avaliação do impacto;
3. Desenvolvimento do plano;
4. Implementação do plano;
5. Manutenção e atualização.

Capítulo 2: Plano Global de Segurança

Após a análise de risco, a organização deverá desenvolver um plano de segurança para as vulnerabilidades e ameaças identificadas ao nível físico, lógico e dos recursos humanos. A sua implementação levará em consideração todos os riscos e vulnerabilidades identificadas. Esse plano é portanto o documento principal de segurança da empresa

1 Plano de Segurança

Segundo Carneiro (2002), quando se avalia o nível de segurança dos SI numa empresa, é necessário elaborar um plano baseado em padrões de segurança, que integre diversos níveis de controlo e que reduza todos os riscos possíveis e apresente soluções para enfrentar as situações inesperadas ou inevitáveis.

Ainda segundo o autor referido, (idem, ibidem) o plano de segurança:

“É uma estratégia planificada de acções e projectos que devem conduzir um SI e os seus centros de processamento de uma situação inicial determinada (e que tem de ser melhorada) a uma nova situação já melhorada”.

Ferreira, e Alves (1995) defendem que o objetivo da formulação do plano de segurança é “garantir que as atividades críticas da organização sejam restabelecidas e mantidas o mais rapidamente possível a seguir a qualquer desastre ou falha importantes que afetem recursos ou serviços essenciais”.

Segundo Carneiro (2002), a elaboração de um plano de segurança global exige que sejam tidos em conta os seguintes aspetos:

- Sensibilizar todos os executivos da organização sobre as questões de segurança dos SI;
- Analisar e diagnosticar a situação atual no que respeita aos riscos e a segurança dos SI a nível de software, hardware e recursos humanos;
- Elaborar um plano para um programa de segurança, o qual deve contemplar os seguintes aspetos:
 - O plano de segurança destina-se a garantir a integridade e exatidão dos dados;
 - Possibilitar a identificação da informação que é tida por confidencial;
 - Considerar as áreas que se destinem a algum uso exclusivo;
 - Proteger a conservação de todos os ativos de desastres provocados por enganos ou por atos hostis e deliberados;
 - Garantir que a organização possa sobreviver a desastres;
 - Evitar que os órgãos de gestão sejam acusados de negligência ou imprudência.

1.1 Plano de Contingência

O Plano de Contingência destina-se a assegurar a continuidade das atividades críticas da organização entre o acidente e a retoma do pleno funcionamento das atividades, incluindo todos os procedimentos de emergência, descrição das equipas que os executa, informação

facilitadora da execução e indicação dos eventos que despoletam os procedimentos (Ferreira e Alves, 1995).

À elaboração de um plano de contingência deve estar associada a ideia de que não é prático nem realista em termos de custo - eficácia proteger a Organização. E deve ser elaborado após uma análise de risco, de modo a assegurar um funcionamento aceitável em termos de custo – eficiência.

Segundo (Simões, 2004), em situações externas, pode-se recorrer a utilização de instalações de reserva – “ **cold centres**” (instalações alternativas sem equipamento disponível), “ **worm centres**” ou “**hot centres**” (instalações alternativas com equipamento disponível) – deve ser considerada no plano de contingência para o caso de acidentes graves ou catástrofes.

Para Silva, Carvalho e Torres (2003), nestes planos deve ser incluídos procedimentos para todas as ações de emergência, incluindo:

- Evacuação;
- Primeiros socorros;
- Redução de danos (por exemplo, extinção de fogo);
- Contenção do incidente (por exemplo, desativação de sistemas);
- Avaliação de danos;
- Escalada e ativação do plano de gestão de crise.

O plano de contingência deve descrever as equipas responsáveis pela execução de cada um destes procedimentos, indicando para cada equipa a sua designação oficial, constituição, estrutura hierárquica, a lista dos meios de que dispõe (diagramas, contactos, procedimentos, etc.) e planos de testes e exercícios, bem como de contactos para comunicação com outras equipas e centros de coordenação. (Silva, Carvalho e Torres, 2003) Para além dos elementos

referidos, o plano de contingência deverá incluir um plano de ação composto por um diagrama de execução (ver Fig.7).

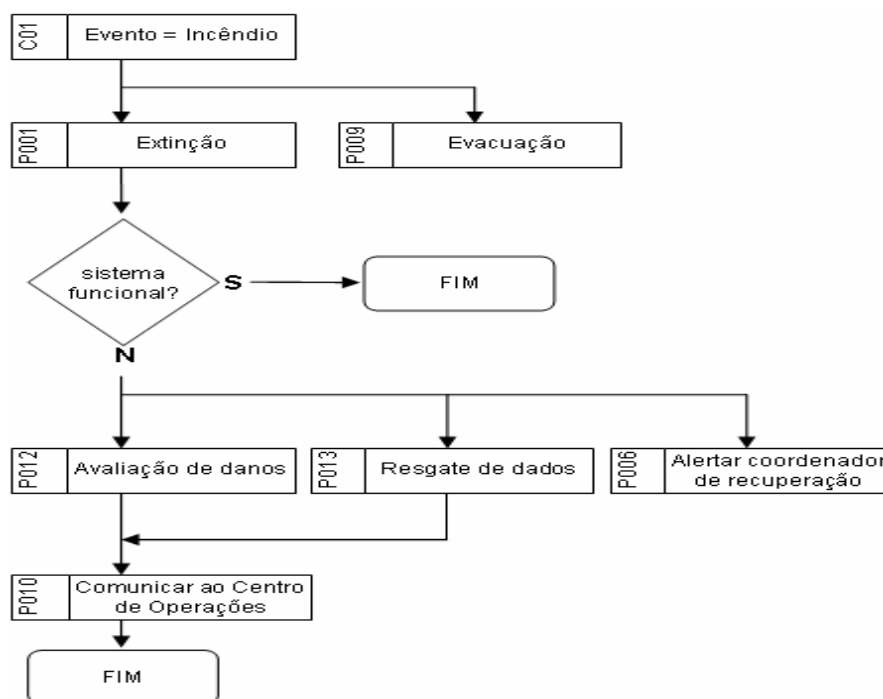


Figura 7: Diagrama de execução

Fonte: Manual Técnico de Segurança dos Sistemas e Tecnologias de informação

O plano de contingência deverá incluir também uma matriz de responsabilidades que permita identificar os procedimentos a executar, quem os executa e quando.

1.2 Plano de Recuperação

Para Silva, Carvalho e Torres (2003), o plano de recuperação é um documento composto pelas descrições das respostas a uma interrupção nas atividades, processos e funções importantes do negócio, que se prolongue para além das respetivas tolerâncias à indisponibilidade.

O plano de recuperação deverá incluir a estrutura e constituição das equipas que deverão executar, o plano de ação e todas as informações auxiliares que facilitem a implementação dos procedimentos (por exemplo, contratos e listas de contactos), englobando a recuperação de (Silva, Carvalho e Torres, 2003):

- Sistemas;
- Dados;
- Comunicações (de dados e de voz);
- Processos TI e não tecnológicos (logística de matéria prima, etc.);
- Postos de trabalho.

Para além destes, deverão ser elaborados ainda procedimentos para o processo de comunicação externa (designada notificação), interna (designada de ativação) e de declaração do desastre aos fornecedores de serviços de recuperação e de suporte (deslocação de pessoal e equipamento, etc.).

1.3 Plano de Reposição

O Plano de Reposição consiste em estabelecer normas que permitam repor o funcionamento do sistema em caso de interrupção ou avaria (Ferreira e Alves, 1995).

Deve estar sempre disponível para fazer face às situações de interrupção ou avaria do sistema.

Segundo o mesmo autor (idem) o plano de reposição pode aplicar-se em caso de ocorrência de incidentes do tipo:

- Avarias no equipamento;
- Avarias de climatização ou de energia elétrica;
- Destruição de ficheiros;

O objetivo principal deste plano é criar cópia de segurança de toda a informação relevante. Para tal deve-se seguir um conjunto de procedimentos e Ferreira e Alves (1995) citam os seguintes que devem ser estabelecidos pelo responsável pelo sistema informático:

- Periodicidade das cópias de segurança: a periodicidade das cópias pode ser diária, semanal, mensal, anual, ou de periodicidade variável;
- Número de exemplares das cópias de segurança;
- Localização de arquivos de suporte de suporte magnético: a localização do armazenamento das cópias de segurança, deve ser feita tendo em conta não só a segurança, mas também a disponibilidade, sempre que haja condições essas cópias devem ser guardadas em lugar distinto dos dados originais;
- Procedimentos de reposição.

Conforme Rosa (2004), existem igualmente outros documentos de segurança que contribuem para dar consistência e exequibilidade às medidas implementadas:

- Política de segurança;
- Normas de Segurança;
- Procedimentos.

1.4 Política de Segurança

A política de segurança pode trazer ao ambiente de uma instituição, regras e procedimentos que devem ser seguidos para a garantia da segurança da informação. É importante que as informações da política de segurança sejam divulgadas para todos os membros da instituição, funcionários, colaboradores ou estagiários, e que todos estejam conscientes da importância do seguimento desta política (Spancesci, 2004).

Para Rosa (2004), política de segurança é um conjunto reduzido de regras que definem em linhas gerais o que é considerado pela empresa como aceitável ou inaceitável, contendo referência às medidas a impor aos infratores.

Na perspectiva de Carneiro (2002), as políticas de segurança "incluem documentos que descrevem, principalmente, a forma adequada de utilização dos recursos do SI, as responsabilidades e direitos tanto dos intervenientes (utilizadores, administradores), apresentam o que devem ser protegidos e descrevem os procedimentos a manter e desenvolver tudo com o objetivo de garantir a segurança do SI".

Segundo Sousa (2006), o desenvolvimento de uma política de segurança é a base de segurança de informação em uma empresa. Alguns padrões e normas internacionais de segurança foram desenvolvidos por organizações normalizadoras como ISO (Internacional Standards Organization) e a BS (British Standard), como ISO 17799 e a BS 7799.

No entender de Monteiro e Boavida (2000), podem resumir-se as principais regras para a definição de uma boa política de segurança:

- Ser facilmente acessível a todos membros de organização;
- Definir os objetivos de segurança;
- Definir objetivamente todos os aspetos abordados;
- Definir a posição da organização em cada questão;
- Justificar as opções tomadas;
- Definir as circunstâncias em que é aplicada cada uma das regras;
- Definir os papéis dos diversos agentes da organização;
- Especificar as consequências do não cumprimento das regras definidas;

- Definir o nível de privacidade garantindo aos utilizadores;
- Identificar os contactos para esclarecimento de questões duvidosas;
- Definir o tratamento das situações de omissão.

Um dos maiores problemas de segurança nas organizações é a falta de consciência, por parte dos agentes da organização, das ameaças que o sistema e redes estão sujeitos. A política de segurança deverá alertar em termos plausíveis e objetivas – os utilizadores para as questões de segurança (Monteiro e Boavida, 2000).

De uma forma geral, o sucesso da Política de Segurança da Informação adotada por uma organização depende da combinação de diversos elementos, dentre eles, a estrutura organizacional da empresa, as normas e os procedimentos relacionados à segurança da informação e à maneira pela qual são implantados e verificados, os sistemas tecnológicos utilizados, os mecanismos de controlo desenvolvidos, assim como o comportamento de diretores, funcionários e colaboradores.

Segundo Ferreira e Alves (1995), para a formulação da política de segurança deverá ser seguido o modelo a seguir discriminado, na figura 8.

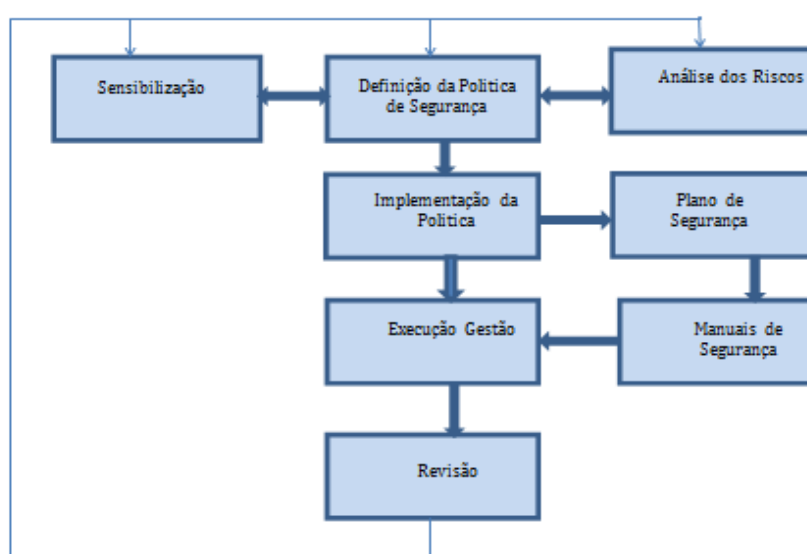


Figura 8: Modelo de formulação da política de segurança, adaptado (Ferreira e Alves ,1995)

A aplicação das medidas de políticas de segurança revelar-se-á tanto mais eficaz quanto duas atividades que precedem a sua formulação ou a acompanham em simultâneo (Sensibilização e Análise de Risco) forem corretamente desenvolvida (Ferreira e Alves ,1995).

1.5 Normas de Segurança

Segundo Rosa (2004), normas de segurança são "documentos composto por todas as regras de segurança da organização concretizando de forma detalhada as orientações da política de segurança. Neste documento são especificadas as tecnologias utilizadas e a forma segura de utilização".

A norma ABNT NBR ISO/IEC 27002:2005, estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Serve como um guia prático para desenvolver os procedimentos e as eficientes práticas de gestão de segurança da informação (ABNT, 2005).

A norma contém 11 seções disponibilizadas em 39 categorias principais que se desdobram em 133 controles.

Os objetivos de controlos definem o que deve ser alcançado em cada categoria descrita nas seções de 5 a 15.

Com isso, a mesma divide-se em:

1) Objetivo

Estabelece as diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização;

2) Temos e definições

Define os diversos termos citados na norma;

3) Estrutura desta Norma

Enumera as seções constantes na norma;

4) Análise/Avaliação e Tratamento de Riscos

Aborda uma noção introdutória de riscos;

5) Política de Segurança da Informação

Provê uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações pertinentes;

6) Organizando a Segurança da Informação

Gerência a segurança da informação dentro da organização;

7) Gestão de Ativos

Mantém a proteção adequada dos ativos da organização;

8) Segurança em Recursos Humanos

Assegura que os funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com os seus papéis, e reduzir o risco de furto ou roubo, fraude ou mau uso de recursos;

9) Segurança Física e do Ambiente

Previne o acesso físico não autorizado, danos e interferências com as instalações e informações da organização;

10) Gerenciamento das Operações e Comunicações

Garante a operação segura e correta dos recursos de processamento da informação;

11) Controle de Acessos

Controla o acesso à informação;

12) Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação

Garante que a segurança é parte integrante de sistemas de informação;

13) Gestão de Incidentes de Segurança da Informação

Assegura que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil;

14) Gestão de continuidade do Negócio

Não permite a interrupção das atividades do negócio e protege os processos críticos contra efeitos de falhas ou desastres significativos, assegura a sua retomada em tempo hábil, se for o caso; e

15) Conformidade

Evita violações de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais e de quaisquer requisitos de segurança da informação.

Com isso, pode-se aplicar a ISO 27002 sem precisar da ABNT NBR ISO/IEC 27001:2006 – Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gestão de Segurança da Informação – Requisitos; mas para se obter a certificação ISO 27001 é necessário ter implantado anteriormente todos os controles recomendados pela ABNT NBR ISO/IEC 27002:2005, conforme figura 9.



Figura 9: ABNT NBR ISO/IEC 27002:2005 - Estrutura (Pompeu, Gledson, 2010)

1.6 Procedimentos

De acordo com Rosa (2004), procedimentos é "o documento que descreve as operações de forma muito detalhada, indicando todos os seus passos. Os procedimentos deverão estar em conformidade com as normas de segurança".

Segundo o procedimento de "logging" num sistema informático deve ser concebido tendo em vista minimizar a oportunidade de acessos não autorizados devendo, por isso, o procedimento de "logon" revelar o mínimo de informações acerca do sistema com o objetivo de evitar fornecer ajudas desnecessárias a um utilizador não autorizado.

Ainda de acordo com o mesmo autor, um bom procedimento de "logon" deverá cobrir os seguintes aspetos:

1. Não visualizar identificadores da aplicação ou do sistema até que o procedimento de logon tenha sido concluído com sucesso;
2. Visualizar um aviso alertando que o sistema apenas pode ser acedido por utilizadores autorizados;
3. Não fornecer mensagens de ajuda durante o procedimento de "logon" que possam orientar um utilizador não autorizado;
4. Desligar e não fornecer nenhuma informação após uma tentativa de "logon" mal sucedida;
5. Validar a informação de "logon" apenas após a conclusão de todos os dados de entrada. Se surgir uma condição de erro, o sistema não deve indicar qual o elemento dos dados que está correto ou incorreto;
6. Limitar o número de tentativas mal sucedidas permitidas antes de ser tomada qualquer ação (três tentativas é o numero recomendado).

Capítulo 3: O Caso INPHARMA

1 Enquadramento

A parte prática visa complementar o tema sobre a Segurança do Sistema de Informação, e consiste num estudo de análise da Segurança dos Sistemas de Informação da Inpharma, tendo em consideração as áreas de segurança de informação, baseada nas melhores práticas do mercado, orientado pelos controlos técnicos da norma ISO/IEC 27002:2005, que rege os padrões internacionais da SI.

A segurança dos sistemas de informação abrange não só a parte lógica da organização, mas também a parte física. Assim, segundo a ISO/IEC 27002:2005, as organizações, seus sistemas de informação e redes de computadores são expostos a diversos tipos de ameaças à segurança da informação, incluindo fraudes eletrónicas, espionagem, sabotagem, vandalismo, roubo, incêndio e inundação, entre muitos outros. O presente estudo de caso visa essencialmente demonstrar que os problemas acima citados podem ser atacados através de soluções de técnicas, mas o seu alcance é limitado, pelo que devem ser também apoiada e reforçada por procedimentos e políticas apropriadas e suportadas pela gestão de topo.

Serão abordadas situações práticas sobre a SSI da Inpharma, baseada nas melhores práticas do mercado. Portanto pretende-se mostrar o quão importante é a implementação de práticas de segurança da informação nas organizações.

2 Apresentação da INPHARMA

Os Laboratórios INPHARMA – Indústria Farmacêutica, SA foi criado a 7 de Janeiro de 1991.

É uma empresa de capital maioritariamente privado, cujo principal objetivo consiste na produção, comercialização e exportação de medicamentos, podendo dedicar-se também a outras atividades afins, conexas ou complementares, incluindo a importação de matérias-primas e subsidiárias, necessárias à sua atividade.



Figura 10: Edifício – Bloco Administrativo dos Laboratórios INPHARMA

Fonte: INPHARMA (2014)

Após a acreditação do Laboratório, a empresa decidiu iniciar e concluir em 2009 o processo de implementação de um sistema de gestão da qualidade de modo a evidenciar um sistema documentado de modo consentâneo com os requisitos da norma NP EN ISO 9001:2008, demonstrando-se em condições de satisfazer os seus clientes e de melhorar continuamente seu

desempenho no âmbito "prestação de serviços de compra logística, distribuição de produtos farmacêuticos e relacionados"¹⁵.

A Inpharma possui um papel chave na sociedade Cabo-Verdiana, favorecendo o acesso de todos aos medicamentos de que necessitem, visando criar riqueza para o país, reduzindo a importação de medicamentos, originando postos de trabalho e gerando lucros.

A figura 8, apresenta um breve resumo histórico da Inpharma.

Datas	Descrição
1991	Constituição da Empresa
1993	Início da Actividade de Produção
1995	Exportação para os Mercados de Angola e Moçambique
2007	Condecoração dos Laboratórios Inpharma com a 1ª Classe da Medalha de Mérito pelo Presidente da República de Cabo Verde
2008	Acreditação do Laboratório de Controlo de Qualidade segundo o Referencial Normativo NP EN ISO/IEC 17025 de 2005
2009	Divisão da Empresa em três Unidades Estratégicas conceptuais: Unidade Fabril, Unidade Não Fabril e InLab (Laboratório de Controlo de Qualidade)
2010	Certificação da Unidade Não Fabril segundo o Referencial Normativo ISO 9001 de 2008 – APCER
2010	Integração do Laboratório de Controlo de Qualidade no conjunto dos Laboratórios de Controlo de Qualidade aceites pela Global Fund
2011	Exportação para os mercados da Guiné-Bissau e S. Tomé e Príncipe
2012	Integração do Laboratório de Controlo de Qualidade no grupo dos Laboratórios pré-seleccionados para realizar serviços na área de avaliação de conformidades de produtos na região da CDEAO
2012	Constituição da Empresa Farmacêutica de São Tomé e Príncipe – Empharma-STP, SA - em parceria com o Governo da República Democrática de São Tomé e Príncipe
2013	Exportação para os mercados da Angola

Figura 11: Historial INPHARMA

Fonte: INPHARMA (2014)

¹⁵ Fonte: http://teste.inpharma.cv/index.php?mod=module&page=2&mod_id=2, consultado a 9 de Junho de 2014.

3 Missão, Visão e Valores

3.1 Missão

A Inpharma orienta a sua missão em produzir medicamentos ao mais baixo custo, com qualidade, eficácia e segurança, contribuindo assim para qualidade da saúde pública, aliada á melhoria permanente e á capacitação para a internacionalização, sustentada numa perspetiva de desenvolvimento da indústria farmacêutica local.¹⁶

3.2 Visão

Para atender e acompanhar as alterações num mundo da globalização a empresa industrial projetou sua visão como:

- Modernização e capacitação empresarial;
- Qualidade e capacitação orgânica;
- Desenvolvimento dos recursos humanos visando uma maior produtividade, através de:
 - Formação;
 - Acesso à informação;
 - Incentivo para um melhor desempenho;
- Demonstração da qualidade: sistema de certificação e acreditação;
- Política comercial pró-ativa;
- Ampliação e modernização da unidade fabril;
- Desenvolvimento tecnológico;

¹⁶ Fonte: http://teste.inpharma.cv/index.php?mod=module&page=4&mod_id=2, consultado a 29 de Abril de 2014.

- Desenvolvimento da gama de produtos;
- Internacionalização seletiva.

3.3 Valores

A Inpharma pauta as suas atividades, tendo em vista os seguintes pontos:¹⁷

- Rigor;
- Qualidade;
- Satisfação dos clientes;
- Satisfação dos colaboradores;
- Ética;
- Espírito de Equipa;
- Cumplicidade.



Figura 12: Missão, Visão, Valores da INPHARMA

Fonte: INPHARMA (2014)

¹⁷ Fonte: http://teste.inpharma.cv/index.php?mod=module&page=4&mod_id=2, consultado a 29 de Abril de 2014.

4 Estrutura Organizacional

A estrutura da Inpharma compreende os seguintes órgãos, como demonstra a figura 13¹⁸:

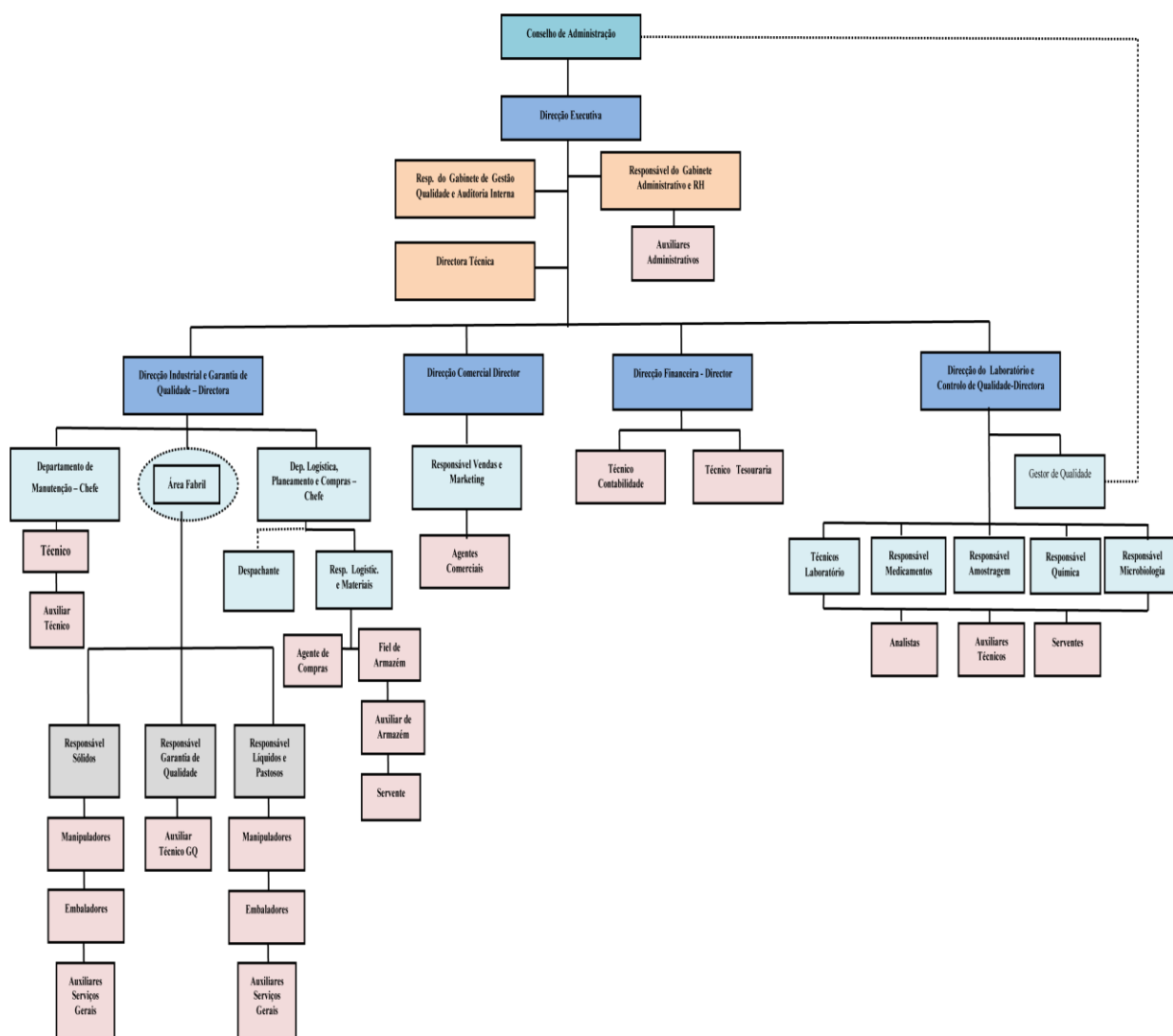


Figura 13: Organograma da INPHARMA

Fonte: INPHARMA (2014)

O Conselho de Administração é Não Executivo, composto pelo Presidente e 2 Administradores. A Direção Executiva é constituída por 4 Diretores das principais Direções

infra referidas. Sendo assim, a empresa possui um total de 62 Colaboradores distribuídos pelas seguintes áreas (Industrial e Garantia de Qualidade, Comercial, Financeira e ainda Laboratório e Controlo de Qualidade).

Segundo a Responsável pelo Gabinete de Recursos Humanos, a Inpharma possui um número de utilizadores superior a 35. Entretanto, o número de técnicos especializados integrados nas equipas de SI é inferior a 2! Assim sendo, a Inpharma subcontratam todo suporte ao SI a empresas especializadas.

É interessante constatar que a totalidade ou as mais importantes funções organizacionais são suportadas pelo SI.

5 Infraestrutura das TIC

Neste capítulo procurou-se saber como é composto os activos de tecnologias e sistemas de informação da Inpharma.

De acordo com o administrador de sistema de informação, ao nível das TIC's e SI a Inpharma possui diversos activos de tecnologias e sistemas de informação, na qual serão apresentados na tabela 3:

Activos de Tecnologias e Sistemas de Informação		
Nome	Marca	Quantidade
Servidores	HP, Asus	6
Desktops	Dell, Toshiba, Tsunami, HP	27
Portáteis	Toshiba, HP	5
Impressoras e Digitalizadores	Brother, HP, Epson, Konica Minolta	10

¹⁸ Fonte: <http://teste.inpharma.cv/uploads/Manual-de-Acolhimento.png/> Consultado a 09 de Junho de 2014

Descrição dos Ativos da TI
Plataforma de Cópias de Segurança (Disco USB, Tapes)
Estrutura de Comunicações & Ativos de Rede (Routers, Access-Points e Switches)
Energia Alternativa/Redundante (Gerador de Energia Elétrica)
Datacenter (Armários, Ar condicionado, Sala e UPS's...)
Serviços externos de website Institucional (Website Corporativo)
Plataforma de Segurança de Perímetro - Firewall (Sistema Operativo, Configurações e Ficheiro)
Plataforma de Controlo de Acessos Web - Proxy (Sistema Operativo, Configurações e Ficheiro)
Partilha de Ficheiros Corporativos e Grupos de Trabalho
Partilha de Ficheiros de Laboratório
Plataforma de Correio Eletrónico
Plataforma Aplicacional Labway e Innovway (base de dados, configurações, ficheiros)
Plataforma de Gestão Documental
Plataforma de ERP Primavera
Plataforma ERP Open ERP
Plataforma ID Presence
Plataforma de Mail Relay Externo (plataforma de receção e filtragem de correio eletrónico)
Domínio Corporativo Inpharma (base de dados, sistema operativo, ficheiros aplicativos (microsoft active directory))

Tabela 4: Activos de tecnologias e sistemas de informação da Inpharma

Segundo o administrador de sistema de informação, existem um total de 6 servidores a funcionarem 24 horas por dia, cuja funções são:

1. **SRVGES** - é um servidor WSUS (Windows Server Update Service), ou seja, serviços de atualizações para todos os servidores e postos de trabalho baseados em Windows. Adicionalmente é também a consola de gestão e updates para o antivírus TrendMicro.

2. **SRVPROXY** - é um servidor proxy web. Faz cache de todos os acessos às páginas Web para minimizar a largura de banda. Adicionalmente faz filtragem de conteúdos.
3. **SRVERP** - é o servidor que possui o software ERP (Sistema Integrado de Gestão Empresarial) desenvolvida para integrar os diversos departamentos da empresa, possibilitando a automação e armazenamento de todas as informações de negócios.
4. **SRVDC** - é o servidor de controlador de domínio principal e com outras funções de DNS Server, Radius Server, File Server. É um servidor de domínio, e-mail e arquivos compartilhados.
5. **SRVFIREWALL** - é um servidor para controlar todos os acessos, internos, externos e VPN na rede de INPHARMA.
6. **SRVDOC** - é o servidor que faz o gerenciamento da plataforma de gestão documental do laboratório, como também serve da plataforma aplicacional do Laboratório Digital.

6 Arquitetura de Rede

O objetivo deste ponto é perceber como é caracterizado a arquitetura de rede Inpharma.

Segundo o administrador de sistema de informação, a arquitetura de rede da Inpharma representada no diagrama da figura 14, é caracterizada por três segmentos de rede, segregados e geridos através dum sistema de controlo de acessos (firewall). A segregação da rede é realizada de forma a agrupar áreas semelhantes e separar sistemas distintos, sendo para isso usados critérios que têm em conta os níveis de segurança e as áreas funcionais. Assim sendo, a arquitetura de rede é constituída pelos seguintes segmentos: rede interna (corporativa); rede visitas; rede pública (Internet).

O segmento de rede “visitas” é destinado a utilizadores temporários ou convidados e é constituída por uma infraestrutura wireless.

A rede pública, é o segmento de rede que está em contacto com a rede Internet, e sobre a qual são desenvolvidos serviços corporativos, como é o caso do correio eletrónico e o acesso remoto à rede interna.

7 Backup & Restauro

O objetivo é conhecer o procedimento de como se efetua o processo de backup. Deste modo procurou-se saber como é efetuado o processo de backup.

De acordo com o administrador de sistema de informação, o processo de backup esta dividido em três componentes:

- **Backups diferenciais diários:** Estão agendados para todas as segundas, terças, quartas e quintas às 23.00h;
- **Backup completo semanal:** Está agendado para todas as sextas às 23.00h;
- **Backup completo mensal:** Está agendado para todas as últimas sextas de cada mês às 23.00h;

De salientar que:

- Os backups diferenciais apenas contempla as modificações dos arquivos que foram alterados desde que foi efetuado um backup completo;
- Os backups são efetuados para o repositório alocado no disco (500GB)
F:\Backup2Disk;
- O restauro dos backups pode ser concretizado através da mesma ferramenta;

- É enviado aos administradores do sistema notificações de alerta via e-mail, como demonstra a figura 15 abaixo;

```
(Server: "SRVDC") (Job: "Backup Diario Disco") The job completed  
successfully. However, the following conditions were encountered:  
  
5 files were skipped.
```

Figura 15: Mensagem de notificação de alerta do estado de backup

Fonte: INPHARMA (2014)

No entanto, segundo o administrador de SI o sistema de backups implementado aquando da reformulação informática realizada no final do ano de 2008, abarcava toda a informação de negócio e informação corporativa considerada importante, e era realizado diariamente com as seguintes características: de segunda a quinta, com retenção de uma semana; sextas com retenção mensal, sendo que a última sexta do mês era retida por sete meses. Este cenário inicial, foi naturalmente sendo alterado no decorrer dos últimos anos, donde destacou-se naturalmente o aumento extraordinário do volume de informação a salvaguardar, e das várias avarias sofridas com o sistema responsável pela componente de backup & restore (de hardware e software). Em maio do ano de 2013, ocorreu uma avaria no sistema de hardware (tapes) que veio limitar grandemente a capacidade de retenção dos backups. Na sequência desse incidente, a política de backups foi adaptada às condições tecnológicas existentes, tendo passado a ser realizado (temporariamente) para um disco externo e da seguinte forma: diário, com retenção de uma semana.

De forma a otimizar a relação custo/benefício, a Inpharma está a definir uma política de backups e adquirir soluções que a possam implementar de forma adequada face às necessidades efetivas da organização.

Neste sentido, sugerimos que é necessário definir uma política de backup & restore de acordo com as necessidades da Inpharma, e reestruturar a atual plataforma tecnológica (com

necessidade de investimento) para a implementação adequada. Entretanto, e no imediato, deverá ser reformulado o plano de backup & restore de forma aumentar a retenção, por exemplo com a alternância de backups totais com backups diferenciais.

Será necessário também que a camada de gestão da Inpharma define o nível de criticidade e capacidade de salvaguarda de cada ativo identificado. Este processo deverá ter como objectivo o estabelecimento da política de segurança – a nível de cópias de segurança (recuperação a desastre e continuidade de negócio) da Inpharma.

8 Medidas de Segurança do SI na INPHARMA

O objetivo deste ponto é conhecer algumas medidas de Segurança do SI, que são aplicadas nesta Instituição.

Segundo o administrador de sistema de informação, a Inpharma aplica as seguintes medidas:

- O acesso à organização é controlado por guardas, que solicitam o documento de identificação de pessoas não autorizado, e faz o registo das entradas e saídas.
- A todos os utilizadores (funcionários, prestadores de serviços) são atribuídos um *username* e uma palavra-chave que são únicas e que não devem ser compartilhadas com qualquer outro colaborador;
- Os utilizadores são solicitados a seguir boas praticas de SI no uso de senhas (as senhas contem oito caracteres no mínimo, incluindo alguns números e caracteres especiais tais como, ! # £ \$);
- As palavras-chave devem ser alteradas em intervalos regulares (45 dias). A equipa de suporte apoia os utilizadores, demonstrando como devem efetuar a alteração da palavra-chave, caso tiverem alguma dificuldade.

- O acesso às aplicações da Inpharma será atribuído tendo em conta as necessidades inerentes ao estatuto dos colaboradores e área de atividade na instituição;
- Não são permitidas atitudes/ações tais como tentativas de acesso não autorizado a dados ou a conta de outro utilizador, ou ainda tentativas de invadir ou sobrecarregar/congestionar deliberadamente a rede;
- Os responsáveis pelo Sistemas de Informação da Inpharma verificam regularmente todos os sistemas e eventuais tentativas de acesso não autorizado aos mesmos. Qualquer tentativa de acesso não autorizado é investigada;
- Nenhum dispositivo periférico (máquinas fotográficas digitais, PDA's, etc.) pode ser instalado ou configurado em qualquer computador da Inpharma, exceto pelo Administrador do Sistema de Informação, com autorização dos Gestores de topo (Direção Executiva);
- A Inpharma faz o controlo de todos os acessos feitos pelos colaboradores a paginas Web e reserva o direito de tornar público o relatório desta informação;
- Não será permitido manter arquivos pessoais, tais como fotos, arquivos de música ou vídeos, nas pastas de partilha de ficheiros corporativos e grupos de trabalho. Exemplo: arquivos. mp3, .avi, .wmv;
- É obrigatório armazenar os arquivos inerentes à instituição no servidor de arquivos para garantir o backup dos mesmos;
- Não é permitida a utilização de serviços de “streaming”, tais como rádios on-line, youtube e afins;
- Os utilizadores não devem visitar paginas de Web que exibam conteúdos de natureza pornográfica, ou que contenham material que possa ser considerado ofensivo;

- Deve-se evitar executar ou abrir mensagens com arquivos anexados enviados por remetentes desconhecidos ou suspeitos, que de alguma forma podem perturbar o normal funcionamento das atividades da organização;
- A atualização do antivírus é feita efetuada de forma automática e centralizada a todos os computadores da rede;
- Os funcionários devem comprometer através de um documento (declaração de confidencialidade) escrito a preservar o sigilo das informações da organização;
- O acesso remoto (o tráfego de informações) deverá ser protegido por VPN, quando se trata de informações confidenciais e críticas para a organização;
- Existe instalado na rede um *software* para detecção de intrusos (IDS) para identificação de qualquer tipo de intrusão que possa prejudicar o normal funcionamento do sistema;
- Os equipamentos são protegidos contra falhas de energia e outras anomalias na alimentação elétrica., utilizando fornecimento de energia permanente como alimentação múltipla, no-break, gerador de reserva, etc.
- Os cabeamentos elétricos e de telecomunicações que transmite dados ou suporta os serviços de informação é protegido contra intercetção ou dano.

9 Análise dos Resultados

A análise dos resultados da Checklist proposta para a verificação dos controlos de segurança, baseada na norma ABNT NBR ISO/IEC 27002, foi efetuada em três fases distintas. Em primeiro lugar verificou-se a análise dos resultados da Segurança Física. Seguidamente realizou-se a análise dos resultados da Segurança dos Recursos Humanos. Numa terceira fase realizou-se a análise dos resultados da Segurança Logica, que foi realizado de forma agrupada

e baseada na seção dos controles de acesso e da seção dos controles de gestão de operações da norma.

As checklist estão divididas em 3 tabelas, apresentadas nos apêndices I, II e III. E os resultados obtidos da checklist são apresentados nos pontos abaixo.

9.1 Segurança Física

A Segurança Física tem como objetivo: prevenir o acesso físico não autorizado, danos e interferências nas instalações e informações. Impedir perdas, danos, furto ou roubo, comprometimento de ativos e interrupção das atividades da organização (ABNT NBR ISO/IEC27002, 2005).

São apresentadas na tabela que se segue os resultados da análise de risco efetuado, tendo em consideração a checklist proposta para verificação da Segurança Física e do Ambiente baseado na norma ABNT NBR ISO/IEC 27002, como demonstra o Apêndice I.

Vulnerabilidade	Impacto	Solução
Possibilidade de intrusão no perímetro físico da empresa, através das falhas do muro inexistente.	Perdas, danos, roubo, comprometimento de ativos e interrupção das atividades da organização	Reforçar os muros de forma a impedir o acesso não autorizado de pessoas.
Utilização de equipamento informático fora das instalações da organização.	Perdas, danos, roubo, comprometimento de ativos e informação.	Deverá ser implementado uma política de utilização dos equipamentos fora das instalações da organização, que carece de autorização superior, coordenação com

		os responsáveis pela gestão dos sistemas de informação e salvaguarda da informação em causa. A proteção da informação contida nos equipamentos pode ser reforçada com controlos de acesso ao equipamento (password BIOS) e encriptação de discos
Possibilidade de intrusão na sala de servidores, através das falhas dos controlos inexistente.	Perdas, danos, roubo, comprometimento de ativos e interrupção das atividades da organização	Acesso controlado a sala dos servidores (por exemplo através de cartões magnéticos, camaras, etc.)
Possibilidade de intrusão na sala de servidores, através das falhas dos registos inexistente.	Perdas, danos, roubo, comprometimento de ativos e interrupção das atividades da organização	Registo de entradas e saídas de pessoas na sala de servidores (por exemplo terminal biométrico)

Tabela 5: Segurança Física

Pelos resultados apresentados na tabela do apêndice I, constata-se que a maioria das medidas de segurança física é aplicada na instituição, como a existência de controlos de entrada para permitir somente a entrada de pessoal autorizado nas instalações da instituição, existência de perímetro de segurança, videovigilância, alarme, guardas com presença permanente, a utilização do UPS para proteção dos equipamentos contra falhas de energia, etc..

Mas no entanto pelos resultados apresentados na tabela 5, verificamos que a segurança física dos equipamentos que são utilizados fora das instalações da organização pode ser melhorada com a introdução de alguns controles adicionais, tais como controles de acesso ao equipamento (password BIOS) e encriptação de discos. Relativamente a possibilidade de intrusão na sala de servidores, através das falhas dos controles inexistente, foi proposto o acesso controlado a sala dos servidores (por exemplo através de cartões magnéticos, camaras, etc.). No que tange a possibilidade de intrusão no perímetro físico da empresa, através das falhas do muro inexistente, pode ser melhorada com o reforço dos muros de forma a impedir o acesso não autorizado de pessoas. Nota-se ainda a possibilidade de intrusão na sala de servidores, através das falhas dos registos inexistente, o que poderá ser solucionada com a utilização de registo de entradas e saídas de pessoas na sala de servidores (por exemplo através terminal biométrico). Portanto a segurança física rigorosa parece carecer de algumas melhorias na Inpharma.

9.2 Segurança com Recursos Humanos

A Segurança dos Recursos Humanos tem como objetivo: assegurar que os funcionários, fornecedores e terceiros entendam as suas responsabilidades para reduzir o risco de erro humano, furto ou roubo, fraude ou mau uso dos recursos. Apoiar a política de segurança da informação na organização durante os seus trabalhos quotidianos. (ABNT, 2005).

A tabela seguinte demonstra o resultado da análise de risco efetuado, tendo em consideração a checklist proposta para verificação da Segurança dos Recursos Humanos baseado na norma ABNT NBR ISO/IEC 27002, como demonstra o apêndice II:

Vulnerabilidade	Impacto	Solução

Possibilidade de contratar pessoas inadequadas a função.	Incidentes de Segurança, como por exemplo: Roubo de equipamentos, Provocação de danos, Conflitos.	Deve ser efetuado pelo RH uma análise cuidadosa dos currículos, do perfil e personalidade, e ainda antecedentes criminais.
Incidentes de segurança como colaboradores ou prestadores de serviços por má conduta, negligência ou falta de informação.	Roubo de Informação; Deterioração de informação ou, Perda de Informação	Os gestores devem garantir que os funcionários e prestadores de serviços estão cientes e motivados para cumprir com as suas obrigações de Segurança de Informação, criando políticas de sensibilização e formação sobre utilização correta do SI, de modo a não por em causa a segurança do mesmo. E devem informar das consequências do não cumprimento das políticas.
Manterem-se ativos acessos e privilégios de utilizadores, colaboradores ou prestadores de serviços mesmo após a cessação de contratos ou funções.	Perda da Informação, Alteração da Informação	Após o término do contrato, prestação de serviços ou alterações de funções, devem ser retirados ou revistos os acessos e privilégios sobre os sistemas.

Tabela 6: Segurança de Recursos Humanos

Relativamente a Segurança dos Recursos Humanos constata-se que a Inpharma aplica diversas medidas de Segurança, como a inclusão em contratos dos termos e condições de emprego e de outros acordos assinados sobre os papéis e responsabilidade de segurança, a aplicação de um processo disciplinar para lidar com violações de segurança de informação, a obrigação de retornar os ativos após a cessação das funções, etc.

Entretanto, a análise da tabela 6 revela, que nem sempre é efetuado uma análise dos currículos e do perfil e adequação do candidato a função a desempenhar. Será necessário reforçar o papel dos gestores, na motivação dos colaboradores e prestadores de serviços na temática da segurança nomeadamente com esclarecimento e controlo do cumprimento das questões relacionadas com a segurança da informação. Constata-se também que existe a possibilidade de contratar pessoas inadequadas a função. Nesse sentido será necessário efetuar uma análise cuidadosa dos currículos, do perfil e personalidade, e ainda antecedentes criminais, pelo RH, como forma de evitar a possibilidade de contratar pessoas inadequadas a função.

De modo a não por em causa a segurança do mesmo as medidas de gestão de recursos humanos carecem dessas melhorias.

9.3 Segurança Logica

A Segurança Logica tem como objetivo: garantir a operação segura e correta dos recursos de processamento da informação; implementar e manter o nível apropriado de segurança da informação; garantir a proteção das informações em rede e da infraestrutura de suporte; prevenir a divulgação não autorizada, modificação, remoção ou destruição dos ativos e interrupções das atividades do negócio, como também controlar o acesso à informação e de utilizadores autorizados, prevenir acesso não autorizado a sistemas e garantir a segurança da informação quando se utilizam os recursos de ambiente de trabalho remoto (ABNT, 2005).

Na tabela que se segue serão apresentados os resultados da análise de risco efetuado, tendo em consideração a checklist proposto para verificação da Segurança Logica baseado na norma ABNT NBR ISO/IEC 27002, como demonstra o apêndice III.

Vulnerabilidade	Impacto	Solução
Informação não protegida	Divulgação não autorizada de informação confidencial, modificação, ou eliminação de informação não autorizada	Implementar uma política de mesa limpa e proteção de informação confidencial, e bloqueio automático de ecrã após um período de inatividade.
Possibilidade da não recuperação das informações no período pretendido	Perda da Informação	Deverá ser Implementado uma política de segurança – a nível de cópias de segurança (recuperação a desastre e continuidade de negócio) da Inpharma, onde a camada de gestão deverá estabelecer o nível de criticidade e salvaguarda de dados para cada ativo (âmbito/abrangência de dados e tempo de retenção). Deverá estabelecer medidas alternativas de recuperação a desastre e continuidade de negócio para os ativos de maior criticidade para o negócio da Inpharma.

Tabela 7: Segurança Logica

Pelos resultados apresentados na tabela do apêndice III, constata-se que a Inpharma aplica a maioria das medidas de segurança lógica nos Sistemas de Informação, como utilização de sistemas de firewall, filtragem de conteúdo, realização de cópias de segurança regulares, utilização de controlos contra códigos maliciosos (antivírus), utilização de controlos criptográficos, controlo de conexão a rede, restrição de acesso a informação, uso de sistema de monitoração, etc.

Mas no entanto, a análise da tabela acima, revela ainda a possibilidade de melhoria da Segurança lógica, com a aplicação da política de mesa limpa e bloqueio de ecrã por parte dos utilizadores, como também a aplicação de uma política de segurança – a nível de cópias de segurança (recuperação a desastre e continuidade de negócio). Nesse sentido, foi proposto a implementação dessas políticas, como forma de solucionar essas falhas.

10 Proposta de Política Mesa Limpa e Proteção de Ecrã

Dada a inexistência de uma política de segurança de mesa limpa e proteção de ecrã na INPHARMA, a proposta vai no sentido de apresentar uma politica baseada na norma da ISO/IEC 17799.

A política de "Mesa limpa e Proteção de Ecrã" tem como objetivo: definir diretrizes que reduzam os riscos de acesso não autorizado, do roubo de informações ou da alteração de informações durante e fora do horário de expediente, causados por documentos que possam ser deixados sozinhos nas instalações da empresa, ou por descuido do utilizador (ISO 27001/17799).

Nesse sentido, a Inpharma deve considerar a adoção de uma política de “mesas limpas” para a informação em suporte de papel e igualmente uma política de “bloqueio de ecrã”, que proteja contra o perigo de usurpação de sessões autenticadas em computadores momentaneamente sem utilizadores.

Esta política aplica-se a todos os utilizadores que têm acesso a qualquer sistema ou tecnologia de informação que pertença ou seja manipulado na Inpharma, sendo eles: funcionários, estagiários, prestadores de serviços ou terceiros devidamente autorizados.

Os seguintes controlos devem ser considerados:

- Sobre a mesa e na área de trabalho dos colaboradores, não deve ser deixada informação confidencial acessível a pessoas não autorizadas. Esta situação assume maior importância nos intervalos de ausência, como a pausa para almoço ou no final do dia. A informação confidencial deve ser guardada em armário fechado, ou cofre, conforme o caso.
- Todos os resíduos de papel, que contenham informações pessoais ou dados confidenciais, devem ser processados de forma a assegurar a proteção da informação, nomeadamente com a sua destruição (rasgar ou triturar). Este tipo de resíduos de papel não deve ser jogado fora como o lixo normal nas caixas de papel usado;
- Sempre que os utilizadores saírem do posto de trabalho e o PC estiver ligado, é essencial que eles bloqueiam o ecrã pressionando 'Ctrl, Alt, Delete' e então entrar, para confirmar que pretendem "bloquear" o posto de trabalho;
- Os computadores, e as impressoras devem ser desligados quando não estão em uso, ou devem ser protegidos por bloqueios, senhas e afins;
- O sistema de bloqueio de ecrã, deve estar protegido com palavra passe, e deve estar configurado para que o bloqueio surja de forma automática e após alguns minutos (entre cinco a dez minutos) de inatividade;
- Informações sensíveis ou confidenciais, quando impressas, não podem ser esquecidas nas impressoras, devem ser retiradas assim que impressas.

Caso os procedimentos ou normas aqui estabelecidos sejam violados, a direção da Inpharma se reserva o direito de aplicar as punições cabíveis aos utilizadores responsáveis pela violação da política.

É importante que após a detecção de violação das normas de segurança estabelecidas na política de segurança, deve determinar se a violação foi causada de forma intencional ou não. Aos utilizadores que de forma intencional violarem as regras de política de segurança, ficam automaticamente bloqueado o acesso ao sistema da organização e serão aplicadas as seguintes sanções: advertência escrita, e em último caso, a demissão. Por outro lado, aos utilizadores que, de forma não intencional desrespeitarem as normas de segurança estabelecidas nesta política de segurança, serão aplicadas as seguintes sanções: advertência verbal, comunicando a norma que foi violada e em último caso, será bloqueado o acesso ao sistema da organização.

11 Proposta de Política de Sensibilização e Formação

Tendo em consideração a inexistência de uma política de sensibilização e formação na Inpharma, a proposta vai no sentido de apresentar uma política baseada na norma da ISO/IEC 17799.

A política de "Sensibilização e Formação" tem como objetivo: assegurar que os utilizadores se conscientizem das preocupações e ameaças à segurança das informações, e minimizar os danos resultantes de incidentes de segurança e mal funcionamentos, e monitorar e aprender com tais incidentes. (ISO 17799).

Esta política aplica-se a todos os utilizadores que têm acesso a qualquer sistema ou tecnologia de informação que pertença ou seja manipulado na Inpharma, sendo eles: funcionários, estagiários, prestadores de serviços ou terceiros devidamente autorizados.

Os seguintes controlos devem ser considerados:

- Os funcionários devem comprometer através de um documento escrito e aprovada pela camada de gestão a preservar o sigilo das informações da organização;

- Todos os utilizadores dos recursos tecnológicos da organização deverão receber ações de formação/sensibilização nos procedimentos de segurança e no uso correto dos equipamentos;
- Todos os utilizadores devem estar conscientes da possibilidade de ocorrência de incidentes como ameaças, falhas que possam ter impacto no funcionamento das atividades da organização;
- Todas as regras e procedimentos de segurança devem ser documentados e divulgados a todos os utilizadores que beneficiam do uso do sistema;
- O responsável de segurança deverá supervisionar todos os utilizadores, certificando-se do uso e implementação de regras básicas de segurança, com especial atenção para os colaboradores novos ou inexperientes;
- Deverá ser estabelecido um processo disciplinar formal para fazer face a violação de políticas e procedimentos de segurança existentes na organização;
- A demissão de um funcionário deve ser acompanhada pela desativação de todos os acessos deste utilizador a qualquer recurso da organização, para evitar posterior acesso a informações da organização.

Caso os procedimentos ou normas aqui estabelecidos sejam violados, a direção da Inpharma se reserva o direito de aplicar as punições cabíveis aos utilizadores responsáveis pela violação da política.

É importante que após a deteção de violação das normas de segurança estabelecidas na política de segurança, deve determinar se a violação foi causada de forma intencional ou não. Aos utilizadores que de forma intencional violarem as regras de política de segurança, ficam automaticamente bloqueado o acesso ao sistema da organização e serão aplicadas as seguintes sanções: advertência escrita, e em último caso, a demissão. Por outro lado, aos utilizadores que, de forma não intencional desrespeitem as normas de segurança estabelecidas nesta

política de segurança, serão aplicadas as seguintes sanções: advertência verbal, comunicando a norma que foi violada e em último caso, será bloqueado o acesso ao sistema da organização.

12 Proposta de Política de Manutenção e Utilização dos Equipamentos

Devido a inexistência de uma política de segurança de manutenção e utilização de equipamentos na INPHARMA, a proposta vai no sentido de apresentar uma politica baseada na norma ISO/IEC 17799.

A política de "Manutenção e Utilização de Equipamentos" tem como objetivo: impedir perda, danos ou comprometimento de ativos e interrupção das atividades do negócio para assegurar sua disponibilidade e integridade continuadas. (ISO 17799).

Os seguintes controlos devem ser considerados:

- Os utilizadores devem estar informados sobre a correta utilização dos equipamentos;
- Os equipamentos devem passar por manutenção de acordo com os intervalos e especificações de serviço recomendados pelo fornecedor;
- Apenas pessoal autorizado de manutenção deve executar os reparos e a manutenção nos equipamentos;
- O suporte só poderão ser prestados por técnicos especializados na área, deverá existir uma equipa técnica interna ou prestadora de serviços disponível para eventuais necessidades.
- As falhas nos equipamentos devem ser registadas em lugar específico para tal, para uma mais rápida resolução de ocorridas ou suspeitadas e sobre todas as manutenções preventivas e corretivas;
- Controles apropriados devem ser realizados quando se enviar equipamento para fora da organização para manutenção;

- Os equipamentos devem ser protegidos contra falhas de energia e outras anomalias na alimentação elétrica utilizando-se para além de UPS, também geradores evitando a indisponibilidade dos serviços.
- Deverá existir monitorização das condições ambientais (proteção contra humidade, calor, poeira, ou outro fator que possa causar dano nos equipamentos) nas salas onde se encontram recursos tecnológicos particularmente nos que guardam informações críticas.
- A utilização dos equipamentos fora das instalações da organização, deverá carecer de autorização superior, coordenação com os responsáveis pela gestão dos sistemas de informação e salvaguarda da informação em causa;
- As instruções dos fabricantes para proteção dos equipamentos devem ser sempre observadas, por exemplo proteção contra exposição a campos eletromagnéticos intensos;
- Equipamentos e mídias retirados do prédio da organização não devem ser deixados desacompanhados em locais públicos. Em viagens, os computadores portáteis devem ser transportados como bagagem pessoal e disfarçados onde possível.

Caso os procedimentos ou normas aqui estabelecidos sejam violados, a direção da Inpharma se reserva o direito de aplicar as punições cabíveis aos utilizadores responsáveis pela violação da política.

Aos utilizadores que de forma intencional violarem as regras de política de segurança, ficam automaticamente bloqueado o acesso ao sistema da organização e serão aplicadas as seguintes sanções: advertência escrita, e em último caso, a demissão. Por outro lado, aos utilizadores que, de forma não intencional desrespeitarem as normas de segurança estabelecidas nesta política de segurança, serão aplicadas as seguintes sanções: advertência verbal, comunicando a norma que foi violada e em último caso, será bloqueado o acesso ao sistema da organização.

Conclusão

O presente trabalho, leva-nos a concluir que de uma forma geral, a INPHARMA aplicam a maioria das medidas de segurança de Sistemas de Informação, como a existência de controlos de entrada para permitir somente a entrada de pessoal autorizado, existência de perímetro de segurança, videovigilância, alarme, utilização de sistemas de firewall, realização de cópias de segurança regulares, utilização de controlos contra códigos maliciosos (antivírus), restrição de acesso a informação, uso de sistema de monitoração, a inclusão em contratos dos termos e condições de emprego e responsabilidade de segurança, a aplicação de um processo disciplinar para lidar com violações de segurança de informação, a obrigação de retornar os ativos após a cessação das funções, e ainda realização de testes e auditorias internas para avaliar o nível de proteção.

Nesse sentido, isto permite concluir que o nível de segurança da INPHARMA atinge um patamar satisfatório, apesar que ainda existem medidas que carecem de melhorias, tais como a implementação de uma política de mesa limpa e proteção de informação confidencial, e bloqueio automático de ecrã após um período de inatividade, a implementação de uma política de utilização dos equipamentos fora das instalações da organização, e ainda o desenvolvimento de um plano de recuperação das funções críticas em caso de desastres (estabelecer medidas alternativas de

recuperação a desastre e continuidade de negócio para os ativos de maior criticidade para o negócio da INPHARMA).

Foi notório que independentemente das medidas preventivas, tecnológicas ou processos implementados na organização, é garantido que existirá uma falha de segurança algures no tempo. Assim, é fundamental uma rápida deteção e resposta ao eventual incidente, valorizando a componente de deteção numa abordagem de segurança corporativa. Nesse sentido uma deteção eficaz é preponderante para a manutenção do nível de segurança de uma organização garantindo a disponibilidade e competitividade do negócio em causa.

Concluimos igualmente que faz-se necessário a implementação de uma política de segurança da informação na INPHARMA que tem por objetivo definir procedimentos, e especificando funções que devem ser seguidas pelos colaboradores da organização. Mas no entanto não basta ter uma política de segurança escrita, se não for aplicada e apoiada pela administração ou se os colaboradores não possuem conhecimento dela.

Reforçamos o facto de seguir uma norma ISO/IEC 27002 é meramente uma boa prática a seguir, mas que deverá ser sempre enquadrada com as necessidades e exigências do modelo de negócio da Organização. Mas no entanto, essa norma foi de muita utilidade e trouxe maior eficiência no decorrer desse processo, pois possibilitou uma análise profundo dos controlos e através desta foi possível propor medidas de melhorias a SSI da INPHARMA.

Bibliografia

ABNT. (2005). *Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação*. Rio de Janeiro.

ABNT. (2008). *Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança da informação*.

ANAC. (2014). *Certificação digital – brevemente uma realidade em Cabo Verde*. Disponível em http://www.anac.cv/index.php?option=com_content&view=article&id=143%3Anoticia-de-teste&catid=35%3Anoticias-banner&lang=pt, Consultado a 17 de Junho de 2014.

Back, J. P. S. (2013). *A importância dos Back-Ups*. Disponível em <http://seginfoatual.blogspot.com/2013/12/a-importancia-dos-back-ups.html>, Consultado a 23 de Maio de 2014.

Beal, A. (2005). *Segurança da Informação: princípios e melhores práticas para a proteção dos ativos de informação das organizações*. Atlas, São Paulo.

Carneiro, A. (2002). *Introdução à Segurança dos Sistemas de Informação*. FCA, Lisboa.

CNASI. (2012). *Ameaças á Segurança da Informação de uma corporação*. Disponível em <http://www.cnasi.com.br/ameacas-a-seguranca-da-informacao-de-uma-corporacao/>, Consultado a 20 de Abril de 2014.

Downing, C. (2001). *Dicionário de termos informáticos e da internet*. Paralelo, Lisboa.

Ferreira, F. Araújo, M. (2006). *Política de segurança da informação: Guia prático para embalagem e implementação*. C. Moderna, Rio de Janeiro.

Ferreira, J. Alves, S. (1995). *Manual Técnico de Segurança dos Sistemas e Tecnologias de Informação*. FCA - Editora de Informática.

IMA. (2014). *Política de Segurança da Informação*. Disponível em <http://www.ima.sp.gov.br/politica-de-seguranca-da-informacao>, Consultado a 19 de Junho de 2014.

INPHARMA (2014). *História da Inpharma*. Disponível em <http://teste.inpharma.cv/>, Consultado a 9 de Junho de 2014.

INPHARMA (2014). *Organigrama da Inpharma*. Disponível em <http://teste.inpharma.cv/uploads/Manual-de-Acolhimento.png>, Consultado a 9 de Junho de 2014.

ISO/IEC 17799 (2001). *Tecnologia da Informação - Código de Prática para Gestão da Segurança de Informação*. Disponível em <http://www.procedimentosemti.com.br/downloads/NBR17799>, Consultado a 2 de Setembro de 2014.

Mamede, H. (2006). *Segurança Informática nas Organizações*. FCA. Lisboa.

Medeiros, C. D. R. (2001). *Segurança da informação – Implantação de medidas e ferramentas de segurança da informação*.

Monteiro, E. Boavida, F. (2000). *Engenharia de redes informáticas*. FCA, Lisboa.

Moraes, A. F. (2010). *Segurança em Redes Fundamentos*. (1ª edição), São Paulo.

Oliveira, W. (2000). *Técnica para Hackers - soluções para segurança*. C. Atlântico, Lisboa.

Rosa, B. I. (2004). *Segurança dos Sistemas de Informação na Cidade da Praia.*, Disponível em <http://bdigital.cv.unipiaget.org:8080/jspui/handle/10964/241>, Consultado em 20 de Abril de 2014.

Salgado, I. J.C, Bandeira, R., Silva, R. S. (2004). *Análise de segurança física em conformidade com a norma ABNT NBR ISO/IEC 17799*.

Santos, V. (2010). *Sistemas de Detecção de Intrusões (IDS – Intrusion Detection Systems) usando unicamente softwares Open Source*. Disponível em

<http://www.seginfo.com.br/sistemas-de-deteccao-de-intrusoes-ids-intrusion-detection-systems-usando-unicamente-sofwares-open-source/>, Consultado a 23 de Maio de 2014.

Silva, M., A., Alberto, N., R. (2003). *Comercio Eletrónico na Internet*. LIDEL, Lisboa.

Silva, F. Q. (1999). *Segurança de Dados*. Disponível em <http://www.aedb.br/seget/artigos11/32614346.pdf>, Consultado em 24 de Junho de 2014.

Silva, P. T., Carvalho, H., Torres, C. B. (2003). *Segurança dos Sistemas de Informação: Gestão Estratégica da Segurança Empresarial*. Centro Atlântico, Lisboa.

Simões, J. (2004). *Segurança de Sistemas Informáticos*.

Sousa, B. L. (2006). *TCP/IP Básico Conectividade em Redes, Dados*. (3ª edição)

Spancesci, F. R. (2004). *Política de Segurança da Informação – Desenvolvimento de um Modelo voltado para instituições de ensino*. Disponível em http://www.mlaureano.org/aulas_material/orientacoes2/ist_2004_francini_politicas.pdf, Consultado a 19 de Junho de 2014.

Anexo

A.1 Declaração de Confidencialidade INPHARMA

 a qualidade na saúde	DECLARAÇÃO DE CONFIDENCIALIDADE	Revisão nº: Procedimento nº: Data: 04/02/2013
---	--	---

DECLARAÇÃO DE CONFIDENCIALIDADE

Eu, _____, portador(a) do Bilhete de Identidade nº _____, emitido em __/__/____ pelo Arquivo Nacional de Identificação Civil e Criminal de _____, residente em _____, possuindo habilitações académicas _____, a exercer funções de _____ na _____ dos Laboratórios Inpharma, SA, declara, sob compromisso de honra, guardar segredo profissional relativamente a todos os factos de que tenha conhecimento no decorrer do exercício das suas funções, obrigando-se a manter o sigilo após eventual cessação de funções, por qualquer motivo.

Apêndices

I. Checklist proposto para verificação da Segurança Física baseado na norma ABNT NBR ISO/IEC 27002

CHECKLIST PROPOSTO PARA VERIFICAÇÃO DA SEGURANÇA FÍSICA BASEADO NA NORMA ABNT NBR ISO/IEC 27002				
Item	Secção	Questões a auditar	Respostas	
			Sim	Não
1	Segurança Física e do Ambiente			
1.1	Áreas de Segurança			
1.1.1	Perímetro de segurança física	As barreiras físicas, como recursos de segurança, foram implementadas para proteger o serviço de processamento da informação.	*	
		Alguns exemplos de tais recursos de segurança são o controlo por cartão do portão de entrada, presença de um funcionário na receção, etc.	*	
1.1.2	Controles de entrada física	Existem controlos de entrada para permitir somente a entrada do pessoal autorizado na sala específica para os servidores.		*
		As salas, que possuem o serviço de processamento de informação, contêm armários fechados ou cofres trancadas.	*	
		Existem registo de entradas e saídas de pessoas na sala dos servidores		*
1.1.3	Segurança em escritórios, salas, e instalações de processamento	O serviço de processamento de informação é protegido contra desastres (incendio) causados pelo homem.	*	
		Há alguma ameaça potencial de propriedades vizinhas.		*
1.1.4	Trabalhando em áreas seguras	Existe algum controle de segurança para prestadores de serviço ou funcionários trabalhando em área de segurança. A informação só deve ser fornecida quando necessário.	*	
1.1.5	Isolamento das áreas de expedição e cargas	As áreas de expedição e carga e de processamento de informação são isoladas uma da outra, para evitar acesso não autorizado.	*	
		Foi realizada uma avaliação de risco para determinar a segurança de tais áreas.	*	
1.2	Segurança dos Equipamentos			
1.2.1	Instalação e proteção dos equipamentos	Os equipamentos são instalados em local apropriado para minimizar acesso não autorizado à área de trabalho.	*	
		Se os itens que requerem proteção especial foram isolados para reduzir o nível geral de proteção exigida.	*	
		Os controlos foram adotados para minimizar o risco de ameaças potenciais, como roubo, fogo, explosão, água, poeira, vibração, interferência no fornecimento de energia, radiação eletromagnética, inundação.	*	
		Se os aspetos ambientais são monitorados para evitar condições que possam afetar de maneira adversa a operação das instalações de processamento da informação.	*	

1.2.2	Fornecimento de energia	Os equipamentos são protegidos contra falhas de energia e outras anomalias na alimentação elétrica., utilizando fornecimento de energia permanente como alimentação múltipla, no-break, gerador de reserva, etc.	*	
1.2.3	Segurança do cabeamento	Se o cabeamento elétrico e de telecomunicações que transmite dados ou suporta os serviços de informação é protegido contra intercetção ou dano.	*	
		Se existe algum controle de segurança adicional para informações sensíveis ou críticas.	*	
1.2.4	Manutenção dos equipamentos	Normalmente os equipamentos têm manutenção de acordo com as especificações do fabricante.	*	
		A manutenção é realizada apenas pelo pessoal autorizado.	*	
		Existem registros com as falhas suspeitas ou ocorridas e de toda a manutenção corretiva e preventiva.	*	
		Se os controles apropriados são utilizados quando do envio de equipamentos para manutenção fora da instalação física.	*	
1.2.5	Segurança de equipamentos fora das dependências da organização	Se um equipamento é autorizado pela direção quando necessitar ser utilizado fora das instalações da organização.		*
1.2.6	Reutilização e alienação segura dos equipamentos	Os dispositivos de armazenamento contendo informações sensíveis são fisicamente destruídos ou sobrescritos de maneira segura.	*	
1.3	Controles Gerais			
1.3.1	Remoção de propriedade	Os equipamentos, informações ou software podem ser retirados em adequada autorização.	*	
		São realizadas inspeções regulares para detetar remoção de propriedade não autorizada.	*	
		As pessoas estão cientes que estas inspeções regulares estão sendo realizadas.	*	

II. Checklist proposto para verificação da Segurança dos Recursos Humanos baseado na norma ABNT NBR ISO/IEC 27002

CHECKLIST PARA VERIFICAÇÃO DA SEGURANÇA DE REC. HUMANOS BASEADO NA NORMA ABNT NBR ISO/IEC 27002				
Item	Secção	Questões a auditar	Respostas	
			Sim	Não
1	Segurança dos Recursos Humanos			
1.1	Antes de Emprego			
1.1.1	Funções e Responsabilidades	No processo de recrutamento de funcionários permanentes, contratados e agentes temporários é levado em conta a responsabilidade de segurança.	*	
1.1.2	Blindagem	É efetuado uma análise dos currículos e dinâmicas do grupo no processo de seleção.		*
1.1.3	Termos e condições de Emprego	É incluído em contratos os termos e condições de emprego e de outros acordos assinados sobre os papéis e responsabilidade de segurança	*	
1.2	Durante o Emprego			
1.2.1	Responsabilidade de Gestão	Os gestores garantem que os funcionários e prestadores de serviços estão cientes e motivados para cumprir com as suas obrigações de Segurança de Informação.		*
1.2.2	Conscientização de segurança da informação, educação e formação	É efetuado campanhas de sensibilização, e formação em Segurança do Sistema de Informação.	*	
1.2.3	Processo disciplinar	Existe um processo disciplinar para lidar com violações de segurança de informação	*	
1.3	Rescisão e Mudança do Emprego			
1.3.1	Responsabilidade de Terminação	Obrigações em curso sob as leis de privacidade, termos contratuais, obrigando-se a manter o sigilo após eventual cessação de funções.	*	
1.3.2	Retorno dos ativos	Se há retorno de informações e equipamentos da empresa na posse da pessoa após a cessação das funções.	*	
1.3.3	Eliminação de direitos de acesso	Atualizam os direitos de acesso após eventual cessação de funções		*

III. Checklist proposto para verificação da Segurança Logica baseado na norma ABNT NBR ISO/IEC 27002

CHECKLIST PROPOSTO PARA VERIFICAÇÃO DA SEGURANÇA LOGICA BASEADO NA NORMA ABNT NBR ISO/IEC 27002				
Item	Secção	Questões a auditar	Respostas	
			Sim	Não
1	Segurança Logica			
1.1		Controle de Acesso		
1.1.1	Requisitos de negócios de controle de acesso	O acesso a rede e conexões é restrito.	*	
1.1.2	Gestão de acesso do utilizador	A atribuição de direitos de acesso aos utilizadores é controlada a partir do registo de utilizador inicial	*	
		Acesso privilegiado	*	
		Efetua a gestão de senha de utilizadores	*	
		É efetuado a revisão dos direitos de acesso do usuário e atualizações de direitos de acesso	*	
1.1.3	Responsabilidades do utilizador	Os utilizadores são solicitados a seguir boas práticas de SI no uso de senhas	*	
		Política de mesa limpa e tela limpa		*
		Não compartilhar senha de utilizadores individuais	*	
1.1.4	Controlo de acesso a rede	Política de uso de serviços de rede	*	
		A autenticação do usuário para conexões externas	*	
		Identificação do equipamento em redes	*	
		Diagnóstico remoto e configuração de proteção da porta	*	
		Segregação de rede	*	
		Controle de conexão de rede	*	
1.1.5	Controle de acesso ao sistema operacional	Controle de roteamento de rede	*	
		Fixar procedimentos log-on	*	
		Identificação de utilizador e autenticação	*	
		Sistema de gerenciamento de senhas	*	
		Uso de utilitários de sistema	*	
		Sessão de time - out	*	
1.1.6	Controle de acesso de aplicativos e informações	Limite do tempo de conexão	*	
		Restrição de acesso à informação	*	
		Isolamento de sistemas sensíveis	*	
1.1.7	Trabalho remoto	Os controles de segurança estão implementados para o trabalho remoto	*	
1.1.8	Controle criptográficos	Gestão de chaves	*	
1.3		Gestão de operações		

1.3.1	Proteção contra Malware	Existe controlos contra códigos maliciosos	*	
		E efetuado regularmente atualizações de controlos contra códigos maliciosos.	*	
1.3.2	Backup	As cópias de segurança são efetuadas regularmente conforme a política de backup		*
		As informações podem ser restauradas em adequada autorização.	*	
1.3.3	Loging e monitoramento	O log de auditoria contendo atividades do utilizador, e outros eventos de segurança de informação são mantidos por um período de tempo de modo auxiliar futuras investigações	*	
		Uso do sistema de monitoração	*	
		As informações de log são protegidas contra falsificação e acesso não autorizado	*	
		As actividades do administrador e operadores de registo são registadas	*	
		As falhas de registo são registadas e analisadas	*	
		Os relógios de todos os sistemas de processamento de informação relevante, estão sincronizados com uma fonte de tempo precisa, acordada	*	